Opinnäytetyö (AMK)

Tietojenkäsittely

Tietojärjestelmät

2014

Okko Kotaviita

TILITOIMISTON TIETOTURVAKARTOITUS

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittelyn koulutusohjelma | Tietojärjestelmät

2014 | 45

Pasi Iivonen

Okko Kotaviita

TILITOIMISTON TIETOTURVAKARTOITUS

Opinnäytetyössä suoritettiin tilitoimiston tietoturvatilanteen kartoitus. Työn tavoitteena oli kartoittaa varsinaissuomalaisen tilitoimiston tietoturvan tila ja löydösten perusteella antaa suosituksia yrityksen tietoturvan kehittämiseksi. Kartoituksen muina tavoitteena oli antaa yritykselle keinoja parantaa yrityksen palveluja sekä kohentaa yrityksen kilpailutilannetta.

Teoriaosuudessa selvitettiin kirjanpitoalaan liittyvän lainsäädännön velvoitteet sekä tietoturvaan ja tietoturvakartoitukseen liittyviä käytäntöjä.

Empiirinen osa koostui kyselylomakkeen tekemisestä, joka laadittiin teoriaosuuden perusteella, yrityksessä paikan päällä tehdystä tietoturvakartoituksesta sekä kartoituksen tulosten perusteella yritykselle laadittujen kehitysideoiden antamisesta. Kartoituksen tulokset julistettiin salaisiksi, koska kartoituksessa käsiteltiin arkaluontoista materiaalia.

Tilitoimistoyrityksen tietoturvatilanteen kartoittamiseksi, tulee selvittää yrityksen lainsäädännölliset velvoitteet tiedon suojaamisen näkökulmasta. Kun yrityksen käytössä olevia toimintatapoja verrataan tietoturvallisiksi todettuihin käsittelytapoihin, saadaan selville yrityksen tietoturvan nykytilanne. Tilanteen parantaminen aloitetaan kehittämällä yrityksen toimintaprosesseja tietoturvallisempaan suuntaan.

ASIASANAT:

tietosuoja, tietoturva, tilitoimisto, kirjanpito

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Data Processing | Information systems

2014 | 45

Instructor | Pasi Iivonen

Okko Kotaviita

AN INFORMATION SECURITY AUDIT OF A BOOKKEEPING COMPANY

The aim of this thesis was to audit the information security environment of a bookkeeping company in Finland Proper region, and to recommend ways to improve the information security situation in the company. Other objectives were to improve the company's services, and to provide supportive tools for the company's management, aiming for a better position at the market at the time of depression.

The theoretical part of this thesis was based on a study of investigating of Finnish bookkeeping laws, information security practices and ways to perform information security audit.

The empirical part consisted of creating an information security questionnaire, performing an information security audit at the company's premises, and giving recommendations on how the company could improve its information security environment. Because private information was accessible during the audit, the results of the audit are confidential.

To survey the information security environment of a bookkeeping company, one should first research legislative obligations of the bookkeeping laws. By comparing sound information security practices and information practices used in the company, a company's information security environment can be improved.

KEYWORDS:

Information security, data privacy, bookkeeping

SISÄLTÖ

KUVAT

1 JOHDANTO

Edrward Snowdenin tehtyä vuonna 2013 NSA:n tiedonkeräämiseen liittyvät paljastuksensa, ovat lähes kaikki kuulleet termin tietoturva. Vaikka termi esiintyy vähintäänkin viikoittain mediassa, harva kuitenkaan ymmärtää mistä lopulta on kyse. Kun alaan perehtymättömiltä ihmisiltä kysytään mitä tietoturva tarkoittaa, kuulee vastauksena lähes aina jotain tietotekniikkaan ja varsinkin virustorjuntaan liittyvää. Harva kuitenkin tietää, että tietoturvalla on ollut merkittävä osa ihmiskunnan historiaa kauan ennen kuin tietokoneista osattiin edes unelmoida.

Muinaisina aikoina viestit kirjattiin paperille, pergamentille tai papyrukselle, jonka jälkeen viestinviejä tai lähetti kuljetti viestin vastaanottajalle. Mikäli viestin kuljettaja oli luotettu, oli hyvin todennäköistä, että viesti kulki lähettäjän ja saajan välin niin että viestin sisältö ei joutunut ulkopuolisten käsiin, ja näin viestin luottamuksellisuus oli säilynyt. Mikäli viesti piti välittää pitkän matkan päähän, oli mahdollista että viestinviejää jouduttiin vaihtamaan matkalla. Tällöin viestinvälityskanava ei ollut enää kovin suojattu, joten piti kehittää keino säilyttää viestin sisältö turvattuna. (Miettinen 2002, 3.)

Kun viestiin lisättiin allekirjoitus, pystyivät osapuolet varmistamaan, että viesti oli autenttinen ja kiistämättömästi sen allekirjoittaneen lähettämä. Tosin tällöin piti ensin tietää, minkälainen viestin lähettäjän allekirjoitus todellisuudessa oli. Jos viesti laitettiin kirjekuoreen, joka tämän jälkeen suljettiin ja sinetöitiin sinettivahalla sekä lähettäjän henkilökohtaisella sinetillä, voitiin nähdä oliko viestin sisältö pysynyt eheänä ja luottamuksellisena. Mikäli viesti olisi avattu matkalla, viestin vastaanottaja olisi huomannut heti että sinetti oli rikottu. (Miettinen 2002, 3–4.)

Allekirjoitus, lähetit ja sinetöidyt viestit antoivat viestinnän osapuolille keinot havaita tietoturvaloukkaukset, mutta tällöin viestien sisällöt joutuivat, varotoimista huolimatta, kolmansien osapuolten haltuun. Viestin sisällön suojaaminen salakirjoittamalla hankaloitti viestin sisällön ymmärtämistä. Salakirjoitus voitiin suorittaa klassisilla salakirjoitusmenetelmillä, esimerkiksi Caesar-salakirjoituksella.

Viestin varsinainen sisältö voitiin kätkeä sanomaan myös steganografisesti. Tällä tarkoitetaan sitä, että viesti voitiin kirjoittaa näkymättömällä musteella, muokkaamalla määrätyt merkitykselliset kirjaimet huomaamattomasti tai poimimalla määrätyt sanat viestin sisällöstä, jolloin oikea viestin sisältö paljastui. (Miettinen 2002, 4–5.)

Vaikka tietoturvaan liittyviä sovelluksia on ollut käytössä jo vuosisatoja, jollei tuhansia, niiden asianmukainen käyttö ei ole itsestäänselvyys. Yhdysvaltalainen voittoa tavoittelematon kauppayhdistys Computer Technology Industry Association (CompTIA) teki tutkimuksen vuonna 2013, johon vastasi yli 500 turvallisuusvastuun omaavaa henkilöä. Marraskuussa 2013 julkaistu 11th Annual Information Security Trends -tutkimuksen vastausaineistosta selvisi, että IT-henkilöstöstä 47% mielestä heitä koskettavista uhista inhimilliset virheet ovat kohtalaisen vakava tietoturvauhka. Silti vain 22 % piti inhimillisiä virheitä vakavana uhkana. Saman tutkimuksen mukaan 55 % tietoturvarikkeistä oli ihmistoimien aiheuttamia. Näistä rikkeistä 42 % johtui osaltaan loppukäyttäjien jättämättä noudattamatta ohjeistusta ja käytäntöjä, 41 % johtui osaltaan IT-henkilöstön jättämättä noudattamatta ohjeistusta ja käytäntöjä, 39 % johtui osaltaan ohjelmistoihin ja verkkosivuihin liittyvän turvallisuuskokemuksen puutteista ja 38 % johtui osaltaan IT-infrastruktuuriin liittyvän turvallisuuskokemuksen puutteesta. (CompTIA 2013.)

Luvuista selviää, että pahimmillaan yksi tietoturvarike voi johtua useammasta syystä. Huolestuttavimpana tietona voidaan pitää kuitenkin sitä, että iso osa IT-henkilöstöstä jättää noudattamatta tietoturvakäytäntöjä. On sanottu, että ”tietosuojasta 80 prosenttia on ihmistä ja psykologiaa” (Andreasson ym. 2013, 20). Ottamalla huomioon edellä mainitut asiat, tulee painottaa yrityksen johdon, sekä ohjeistuksen, merkitystä yrityksen tietoturvaan.

Kiinalainen strategi Sun Tzu kertoo teoksessaan Sodankäynnin taito ohjeistuksen noudattamisen tärkeydestä: ”Elleivät ohjeet ole selkeitä ja ellei käskyjä selvitetä perusteellisesti, se on komentajan vika. Mutta kun käskyt on selitetty eikä niitä noudateta, on se sotalain mukaan upseereiden rikos.” (Sun Tzu 2007, 65–66). Esimerkissä seuraavaksi Sun Tzu tosin päästi päiviltä vastuussa olleet up-

seerit, jotka sattumoisin olivat keisarin jalkavaimoja. Tietenkään näin ankariin kurinpitotoimiin ei nykyään voi, eikä tule ryhtyä, mutta työntekijöille tulee saattaa tietoon että ohjeistuksen noudattaminen on avain onnistuneeseen tietoturvaan.

Varsinaissuomalaisella tilitoimistolla oli tarve parantaa omia palveluitaan sekä samalla kartoittaa yrityksen tietoturvan taso. Tarve syntyi kahdesta syystä: tietoturvatietouden lisääntyminen aiheeseen liittyvän uutisoinnin määrän kasvaessa, sekä yrityksen kilpailutilanteen parantaminen heikossa taloustilanteessa. Yrityksen henkilökunnalla ei ollut kuitenkaan riittävää tietoutta kartoituksen laatimiseksi, jolloin sain tilaisuuden suorittaa yrityksen tietoturvakartoituksen.

Tämä raportti toimii yrityksen tietoturvaan liittyvän kehityksen pohjana. Tietoturvaan liittyviä aiheita on yritetty käsitellä mahdollisimman useasta näkökulmasta. Johtamisen tärkeyttä ja johtamiseen liittyviä apuvälineitä on tosin painotettu. Kaikkia asioita ei ole siksi pystytty käsittelemään kovinkaan yksityiskohtaisesti. Ideana onkin ollut herättää ajatuksia siitä, minkälaisia asioita tietoturva voi pitää sisällään, ja että tietoturvassa ei ole kysymys pelkästään virusturvasta ja palomuureista. Tämä koskee varsinkin henkilöitä, joilla ei ole laajaa tietoturvallisuuteen liittyvää kokemusta.

Raportin teoriaosuuden pohjalta laadittu tietoturvakysely on yritetty toteuttaa niin, että vaikka toimeksiantajayrityksen ala on kirjanpito, voidaan kyselyä käyttää eri alojen yritysten tietoturvan kartoittamiseen. Kuitenkin toimeksiantajayrityksen tietoturvan kartoittaminen ja tietoturvan parantamiseen tähtäävien kehitysideoiden antaminen on pääasia.

2 PERUSKÄSITTEET

Aiheena tietoturva on erittäin laaja, joten on välttämätöntä ymmärtää aiheeseen liittyviä peruskäsitteitä. Tässä kappaleessa käsitellään tietoturvaan liittyviä peruskäsitteitä sekä tietoturvan hallintaan liittyviä mekanismeja.

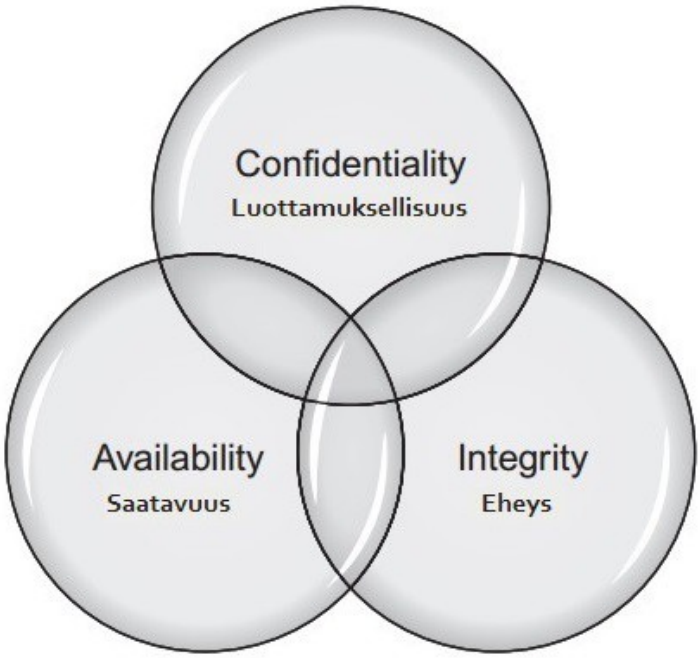
2.1 Tietosuoja ja tietoturva

Tietosuojalla voidaan tarkoittaa henkilötietolain ja erityslakien henkilötietojen käsittelyä koskevien vaatimusten huomioon ottamista yksityisten henkilöiden, eli rekisteröityjen (tietoja säilytetään usein rekistereissä), yksityisyyden suojan ja oikeusturvan varmistamiseksi. Rekisteröity on henkilö, esimerkiksi asiakas, työntekijä tai opiskelija. Näin ollen tietosuojan tarkoituksena on suojata rekisteröidyn yksityiset tiedot, sekä ohjata rekisterinpitäjää hyvien henkilötietojen käsittelytapojen käyttöön. (Andreasson ym. 2013, 14–15.)

Tietoturvalla tarkoitetaan niitä käytännön toimenpiteitä, joiden avulla rekisteröidyn tiedot pysyvät luottamuksellisena, eheinä sekä tarpeen mukaan saatavilla. Päämärän saavuttamiseksi käytetään sekä teknisiä että organisatorisia keinoja (Andreasson ym. 2013, 14).

Kirjassaan The Basics of Information Security – Understanding the Fundamentals, Jason Andress kertoo että tietoturva on tiedon ja järjestelmien suojaamista niiden varalta, jotka haluavat kyseisiä tietoja ja/tai järjestelmiä käyttää vääriin tarkoituksiin. Yleisesti voidaan sanoa, että turvaaminen tarkoittaa varojen suojaamista. Tällä tarkoitetaan, että varat voidaan suojata tietoverkkoa kohdistuvien hyökkäysten, luonnonmullistusten, epäsuotuisien luonnonolojen, sähkökatkojen, varkauksien, ilkivallan tai muita epätoivottuja tapahtumia vastaan. (Andress 2011, 2.)

Lyhyesti ilmaistuna tietoturvan avulla suojataan lain määräämät yksityistiedot. Yritystoiminnan tapauksessa tietoturvalla suojataan kaikki sellainen tieto, jolla on arvoa yritykselle.



Kuva 1: Tiedon kolme ominaisuutta (Andress 2011, 5).

Tietoturvan kolme peruskäsitettä, kuten kuvassa 1 on esitetty, ovat: luottamuksellisuus, eheys ja saatavuus. Englanninkieliset termit näille kolmelle ovat confidentiality, integrity ja availability (niin sanottu CIA-kolmio). Peruskäsitteiden avulla on tarkoitus selvittää tiedon kolme ominaisuutta. Tietoon on oltava pääsy vain niillä henkilöillä, joilla on siihen lupa. Tietoa ei pidä pystyä tarpeettomasti muuttamaan, tapahtukoon muutos tahattomasti tai tahallisesti. Tiedon pitää olla saatavilla kun sitä tarvitaan.

Luottamuksellisuus tarkoittaa siis sitä, että tietoa voivat käyttää vain ne joilla on siihen oikeus. Luottamuksellisuuden voi menettää usealla eri tavalla. Tieto voi joutua vääriin käsiin esimerkiksi hukkaamalla tallennusmedian, ulkopuolinen voi väärinkäyttää urkkimaansa salasanaa, sähköpostia voi lähettää väärään osoitteeseen tai hyökkääjä voi tunkeutua järjestelmiin ja varastaa sieltä tietoa. (Andress 2011, 4–5.)

Eheys tarkoittaa että tieto ei muutu tarkoituksetta tai luvattomasti. Tietoa voi haluta muuttaa, käsitellä tai varastaa jokin ulkopuolinen taho. Joskus tietoon on tarkoitus tehdä jokin muutos, mutta väärät käsittelytavat aiheuttavatkin tietoon

muutoksia, joita ei ollut tarkoitettu tapahtuvan. Eheyttä voidaan suojata erilaisilla suojamekanismeilla, jotka estävät käyttäjiä tekemästä heille toimintoja, joihin heillä ei ole lupa. (Andress 2011, 5–6.) Mikäli tiedon eheys menetetään, voidaan varmuuskopioinnilla sekä versionhallinnalla palauttaa tieto aikaisempaan tilaan. Tällöin kaikki palautuspisteen jälkeen järjestelmään syötetty informaatio pitää tosin syöttää järjestelmään uudelleen.

Saatavuudella tarkoitetaan sitä, että tieto on saatavilla silloin kun sitä tarvitaan. Saatavuuteen voivat vaikuttaa esimerkiksi sähkökatkot ja tietojärjestelmiin liittyvät ongelmat (Andress 2011, 6). Tiedon saatavuuteen voivat vaikuttaa myös tietotekniikkaan liittymättömät asiat, esimerkiksi lukittuun varastoon pääsemättömyys voi estää tärkeän paperidokumentin noutamisen.

CIA-kolmio ei välttämättä kuvaa tietoturvaan liittyviä peruskäsitteitä tarpeeksi laajasti, ja muun muassa Donn Parker on esitellyt kirjassaan Fighting Computer Crime niin sanotun Parkerin kuusikon. Kuusikon pohjana on CIA-kolmio, johon on lisätty kolme lisäkäsitettä, jotka ovat hallussapito (possession), autenttisuus (authenticity) sekä käyttökelpoisuus (utility). (Andress 2011, 25.)

Mikäli jälkikäteen halutaan tarkastella kuka tietoa on käyttänyt tai muuttanut, pitää suojauksessa huomioida myös kiistämättömyys (non-repudiation tai accountability). Kiistämättömyys saavutetaan kirjaamalla käyttäjien tekemisiä loki-tiedostoihin. Lokeihin voidaan kirjata tietoon tehdyn muutoksen ajankohta, sekä käyttäjä joka muutoksen on tehnyt. Kun henkilökunta on tietoinen että heidän toimintaa seurataan, toimii kiistämättömyyteen liittyvät kontrollit pelotteena ja näin ennaltaehkäisevät mahdollisia väärinkäytöksiä. Osaa ihmisistä kyseinen seuraaminen voi ahdistaa, ja tämä tulee ottaa huomioon mikäli seurantaa aletaan suunnittelemaan. (Andress 2011, 53–54.)

2.2 Tietoturvan johtamis- ja hallintajärjestelmä

Jotta yrityksen päättävissä asemissa olevat henkilöt ovat tietoisia yrityksen tietoturvallisuuden tasosta, arvioidakseen yrityksen toimintaan kohdistuvia tietoturvariskejä ja kehittääkseen yrityksen tietoturvan tasoa, tulee yrityksen ottaa käyt-

töön tietoturvallisuuden johtamis- ja hallintajärjestelmä. Järjestelmä koostuu kaikista niistä johtamismenettelyistä, joiden avulla yrityksen tietoturvavaatimuksia johdetaan, ohjataan ja valvotaan. Järjestelmän osia voivat olla yrityksestä riippuen esimerkiksi riskianalyysi, turvallisuusstrategia, tietoturvasuunnitelma ja -ohjeet sekä jatkuvuussuunnitelma. (Valtiovarainministeriö 2007, 13-14; ISO/IEC 27001:fi 2006, 10.) Järjestelmän voi kuvailla olevan enemmänkin kokoelma ohjeita sekä käytäntöjä, kuin tietotekninen järjestelmä.

Tietoturvan hallintajärjestelmien on kehittämiseen on suositettu aikaisemmin Suunnittele-Toteuta-Arvioi-Toimi -mallia, eli PDCA-mallia (ISO/IEC 27001:fi 2006). ISO/IEC 27001:2013 -standardissa tämä malli on muuttunut. Nykyään normaalitilanteista poikkeaviin tapahtumiin tulee reagoida heti kun tapahtuma havaitaan. Tapahtuman aiheuttaja ja tapahtuman aiheuttamat vahingot tulee korjata. Tämän jälkeen tapahtumaan liittyvät tiedot tulee käydä läpi, sekä tulee tutkia voiko sama tapahtuma aiheuttaa haittaa muualla yrityksen toiminnassa. Tarpeen tulleessa tietoturvan hallinta- ja johtamisjärjestelmä tulee päivittää. Lopulta tapahtuman yksityiskohdat sekä korjaavat toimenpiteet dokumentoidaan. (ISO/IEC 27001:en 2013.)

Tietoturvan johtamis- ja hallintajärjestelmän osana, tietoturvakäytännöt ja -periaatteet sisältävät tarkat tiedot siitä minkälaisia kontrolleja yrityksellä on käytössään. Kontrollit voivat olla ohjeistuksen omaisia sääntöjä siitä, miten jokin liikeprosessi tulee suorittaa. Sääntöjä voivat olla esimerkiksi puhtaan työpöydän politiikka, arkaluontoisen materiaalin hävitys turvallisesti sekä ohjeistus sähköpostin turvalliseen käyttöön. Kontrolli voi myös olla fyysinen tai looginen järjestely, joka takaa sen, että liikeprosessi tulee suoritettua oikein. Sisäänkirjautuminen on kontrolli, jolla taataan käyttäjälle riittävät oikeudet järjestelmien käyttöön.

Tietoturvakäytännöt ja -periaatteet -dokumentin sisältö on aina yrityskohtainen. Dokumentti laaditaan yrityksen toimialan sekä koon suhteen. Ohjeistuksen laatimisen apuna voidaan käyttää viitekehyksenä jotakin standardia tai jonkin viranomaisen laatimaa ohjeistusta. Tunnettuja teoksia ovat ISO 27000 -perheen standardit, Valtionhallinnon tietoturvallisuuden johtoryhmän VAHTI-ohjeistus, National Institute of Standard and Technologyn SP 800-160 Systems Security

Engineering – An Integrated Approach to Building Trustworthy Resilient Systems -julkaisu, Bundesamt für Sicherheit in der Informationstechnikin IT-Grundschutz -ohjeistukset, tai tässä työssä käytettävä Information Security Forumin The Standard of Good Practice for Information Security.

2.3 Tietoturvakartoitus

Tietoturvakartoitus tehdään vertaamalla yrityksen nykyisiä toimintatapoja tietoturvallisiksi todettuihin toimintatapoihin. Kartoituksen voi hoitaa yrityksen oma henkilökunta, tai jokin kolmas osapuoli. On tärkeää, että tarkastusta tekevät henkilöt eivät ole osallistuneet järjestelmien suunnitteluun tai käyttöönottoon. (BSI 2008, 11.) Näin tietoturvan tasosta saadaan mahdollisimman neutraali kuva.

Tietoturvakartoituksen tekevän henkilön, tai henkilöiden, tulee päästä käsiksi kaikkeen yrityksen käytössä olevaan tietoon. Lisäksi tarkastuksessa käydään läpi yrityksen liiketoimintaprosessit. Kyseiset seikat aiheuttavat sen, että tarkastuksen kohteena olevalla yrityksellä tulee olla täysi luottamus tarkastusta tekevää ryhmää kohtaan. Asia korostuu varsinkin silloin, mikäli ulkoinen toimija suorittaa tarkastuksen. Ennen kartoituksen tekemistä tulee varmistua siitä, että kartoituksen tekijöillä on riittävä ammatillinen osaaminen, he ovat motivoituneita ja tekevät työnsä perusteellisesti. (BSI 2008, 15.)

Mikäli tietoturvakartoitus tehdään yrityksen sisäisesti, kartoituksesta vastaava henkilö käyttää kartoituksen apuna valmiita kartoitustyökaluja, tai hän voi käyttää pohjana jotakin jo olemassa olevaa työkalua tai kriteeristöä. Ulkopuolinen taho, esimerkiksi tietoturvakonsultti, käyttää vastaavaa työkalua, mutta sen tarkempi sisältö voi olla yrityssalaisuuden suojaama. Kartoitustyökalu on tarkastuslistamuotoinen dokumentti, joka käydään kohta kohdalta läpi. Jokaisen kohtaan merkitään kohdan edellyttämät tiedot mahdollisine erityshuomioineen.

Haavoittuvuus- ja tunkeutumistestauksen avulla voidaan kartoittaa yrityksessä käytössä olevien järjestelmien tietoturvan tilaa. Haavoittuvuustestaukseen voidaan käyttää automatisoituja ohjelmistoja, jotka etsivät järjestelmistä tunnettuja

haavoittuvuuksia. Ohjelmat tuottavat testauksesta raportin johon on kerätty kaikki järjestelmästä löytyneet haavoittuvuudet. Tunkeutumistestauksessa haavoittuvuuksia yritetään käyttää hyödyksi niin, että hyökkääjät pääsevät tunkeutumaan yrityksen järjestelmiin tai pääsevät käsiksi yrityksen tietoihin. (Andress 2011, 59-60.)

Tietoturvatarkastuksen tuloksena saadaan tietoturvan tilasta kertova raportti. Raportti sisältää tietoa yrityksen tietoturvan tasosta. Raportin tietoa voidaan käyttää yritysjohdon apuna, tai tietotekniikasta vastaavat henkilöt voivat tehdä raportin pohjalta muutoksia käytössä oleviin tietoturvakäytäntöihin. (BSI 2008, 11.)

Esimerkkejä työkaluista, kriteeristöistä, viitekehyksistä tai kokoelmista, joita voidaan käyttää tietoturvakartoituksen pohjana ovat muun muassa:

- Kansallinen turvallisuusauditointikriteeristö, KATAKRI versio II
- Valtionhallinnon tietoturvallisuuden johtoryhmän VAHTI-ohjeet
- ISO/IEC 27002 & ISO/IEC 27004 -standardit
- Software Engineering Instituten OCTAVE-menetelmät
- SANS-insituutin Critical Security Controls: Guidelines -ohjeet
- National Checklist Program Repositoryn kautta löytyvät ohjeet
- Santa Fe Groupin SIG-kysymyslista.

3 TIETOSUOJA JA KIRJANPITO

Kirjanpitoon liittyvä lainsäädäntöaineisto löytyy pääpiirteittäin kirjanpitolaista. Kirjanpitolakia tukee muun muassa Kirjanpitoasetus 30.12.1997/1339 sekä Kauppa- ja teollisuusministeriön päätös kirjanpidossa käytettävistä menetelmistä 47/1998. Tietoturvan kannalta mainittavaa on jälkimmäisen päätöksen luvut koneellisten tietovälineiden hyväksikäyttäminen sekä korjausmerkinnän tekeminen. Edellä mainittujen lähteiden sisältämää aineistoa, sekä kirjanpitoon liittyviä elimiä, on käyty tarkemmin läpi tässä osiossa.

Työ- ja elinkeinoministerin alaisuudessa toimii kirjanpitolautakunta, jonka tehtävänä on ohjeiden ja lausuntojen antaminen hakemuksen perusteella kirjanpitolain soveltamisesta, yleisten neuvojen ja ohjeiden antaminen kirjanpitolain soveltamisesta ja kirjanpidon pitämisestä, tarpeelliseksi katsomiensa esitysten tekeminen työ- ja elinkeinoministeriölle sekä lausuntojen antaminen pyynnöstä työ- ja elinkeinoministeriölle (Kirjanpitolautakunta).

Suomen Taloushallintoliitto ry on julkaissut verkkosivuillaan Kirjanpidon ABC:n, jossa käydään läpi mitä asioita kirjanpitolaki velvoittaa käytännössä kirjanpitovelvolliset tekemään. Suomen Taloushallintoliitto ry on omien sanojensa mukaan ”taloushallinnon palveluja tarjoavien auktorisoitujen tilitoimistojen ja konsulttiyritysten valtakunnallinen toimialajärjestö, jonka päämääränä on kehittää tilitoimistoalaa yhdessä jäsenyritystensä kanssa” (Suomen Taloushallintoliitto ry 2009).

3.1 Kirjanpitoaineisto

Kirjanpitovelvollisia ovat kaikki yritykset. Kirjanpidon tehtävänä on pitää kirjaa yrityksen tuloista, menoista, veloista ja varallisuudesta. Kirjanpitoaineistoa ovat kaikki tiedostot ja paperit, jotka kuvaavat yrityksen liiketapahtumia. Kyseisiä dokumentteja kutsutaan tositteiksi. Tositteet voivat siis olla sähköisessä tai paperisessa muodossa. Sähköisiä tositteita ovat muun muassa tiliotetiedostot, tiedostot lähetetyistä laskuista, tiedostot maksettavista laskuista, skannattu ostolasku,

verkkolasku ja muut sähköiset ostolaskut. Paperisia tositteita ovat muun muassa paperilaskut, rahtikirja, tiliote, kuitti käteis- tai korttimaksusta, kassapäätteen tarkkailunauha, liikekirja, eläkevakuutusilmoitus sekä oikeuden päätös. Yritysten välisestä rahaliikenteestä syntyvien tositteiden lisäksi viranomaisilmoitukset, eläkevakuutusilmoitukset sekä muut lainsäädännön määräämät ilmoitukset ovat kirjanpitoaineistoa. (Suomen Taloushallintoliitto ry 2011.)

Muuta kirjanpitoaineistoa ovat muun muassa päivä- ja pääkirjat sekä reskontrat. Päiväkirjassa liiketapahtumat ovat kirjattuna ajan mukaisessa järjestyksessä, pääkirjassa tileittäin. Myyntireskontrasta selviää asiakkaat, joilta ei ole vielä saatu maksusuoritetta. Ostoreskontrasta selviää toimijat, joille yritys ei ole suorittanut omia maksuvelvoitteittaan. (Suomen Taloushallintoliitto ry 2011.)

Tositteen tulee olla selväkielinen ja selkeällä tavalla tehty (Kirjanpitolaki 30.12.1997/1336). Tositteen tärkein tehtävä on todistaa liiketapahtuma, joten tositteesta selvittävä minkälainen liiketapahtuma on ollut kyseessä, sekä tositteen perusteella on pystyttävä laatimaan liiketapahtuman kirjanpitomerkintä. Vaikka tositteiden pitää olla pääsääntöisesti alkuperäisiä, voidaan esimerkiksi kuitti tai lasku skannata kuva- tai pdf-tiedostoksi. Tositteet tulee säilyttää 6 vuotta ja kirjanpitokirjat 10 vuotta tilikauden päättymisen jälkeen. (Suomen Taloushallintoliitto ry 2011.) Lämpökuittien säilytyksessä tulee huomioida alkuperäisen kuitin rajallinen säilyvyys. Parhaimmassa tapauksessa oikein säilytetyn kuitin pitäisi olla luettavissa vuosia. Tosin huonoimmassa tapauksessa kuitti tuhoutuu lukukelvottomaksi hetkessä. (Enfield 2013.)

Tositteesta tulee selvitä luovutus-, lasku- tai maksupäivä, ostotapauksessa mitä ja keneltä on ostettu, myyntitapauksessa mitä ja kenelle on myyty. Maksutositteessa pitää näkyä maksaja, maksun saaja ja maksun syy. Arvonlisäverolaki määrää, että laskussa pitää olla merkintänä muun muassa myyjän arvonlisäverotunniste, myyjän ja ostajan nimi ja osoite. (Suomen Taloushallintoliitto ry 2011.)

Kirjanpitotoiminnassa tarvittavia perustietoja ovat ainakin yhteys-, henkilö-, tilikausi-, ja kaupparekisteritiedot, toimiala, kotipaikka, kansallisuus sekä hallituk-

sen jäsenet. Osapuolten on pidettävä salassa tietoonsa saamansa toisen osapuolen liikesalaisuudet ja muut luottamukselliset tiedot. Tietoja saa käyttää vain sopimuksessa sovittujen ehtojen täyttämiseksi. On huomioitavaa, että salassapito jatkuu myös senkin jälkeen kun osapuolten välinen sopimus päättyy. Sopimuksen päättyessä kirjanpitomateriaalin säilytys ei ole enää tilitoimiston vastuulla. (Suomen Taloushallintoliitto ry 2011.)

3.2 Tietosuojalainsäädäntöä

Henkilötietolaki, sekä laki yksityisyyden suojasta työelämässä, suojaavat yksityishenkilöiden tietoja. Tämä koskee sekä yrityksen omaa henkilökuntaa kuin myös sidosryhmiin kuuluvia henkilöitä. Laki yksityisyyden suojasta työelämässä määrää, että työnantaja saa käsitellä vain työsuhteen kannalta tarpeellisia henkilötietoja. Näiden tietojen tulee liittyä siihen että työnantaja sekä työntekijä voivat hoitaa velvollisuudet toisiaan kohtaan. Näitä vaatimuksia ei voida olla huomioimatta edes silloin, kun työntekijä siihen suostuisi. Työntekijältä on lisäksi kysyttävä lupa, mikäli työnantaja kerää henkilötietoja muista lähteistä. (Laki yksityisyyden suojasta työelämässä 13.8.2004/759.)

Henkilötietolakia sovelletaan aina henkilötietoja käsiteltäessä. Henkilötietoja kerättäessä ei tule kerätä tietoa ihmisten etnisestä alkuperästä, uskonnollisesta tai poliittisesta vakaumuksesta, ammattiliittoon kuulumisesta, sairauksista, sukupuolisesta suuntautumisesta tai käyttääkö henkilö esimerkiksi sosiaalipalveluita. (Tietosuojavaltuutetun toimisto 2014.)

Vaikka yritys olisi tietoinen yleisestä ja alakohtaisesta lainsäädännöstä sekä viranomaismääräyksistä, voi yritysten väliset sopimukset aiheuttaa lisää tietosuojavelvoitteita (Valtiovarainministeriö, 2012).

4 TIETOTURVAN OSA-ALUEET

Tietoturvaan liittyvien asioiden määrän vuoksi, on hyödyllistä jakaa asiat osa-alueiden alle. Valtiohallinnossa on käytössä kahdeksan osa-aluetta. Tietoturva-blogia kirjoittavan Matti Laakson Tietojesi turvaksi -blogista lainattuna, nämä kahdeksan tietoturvan osa-aluetta on perinteisesti jaettu seuraavasti:

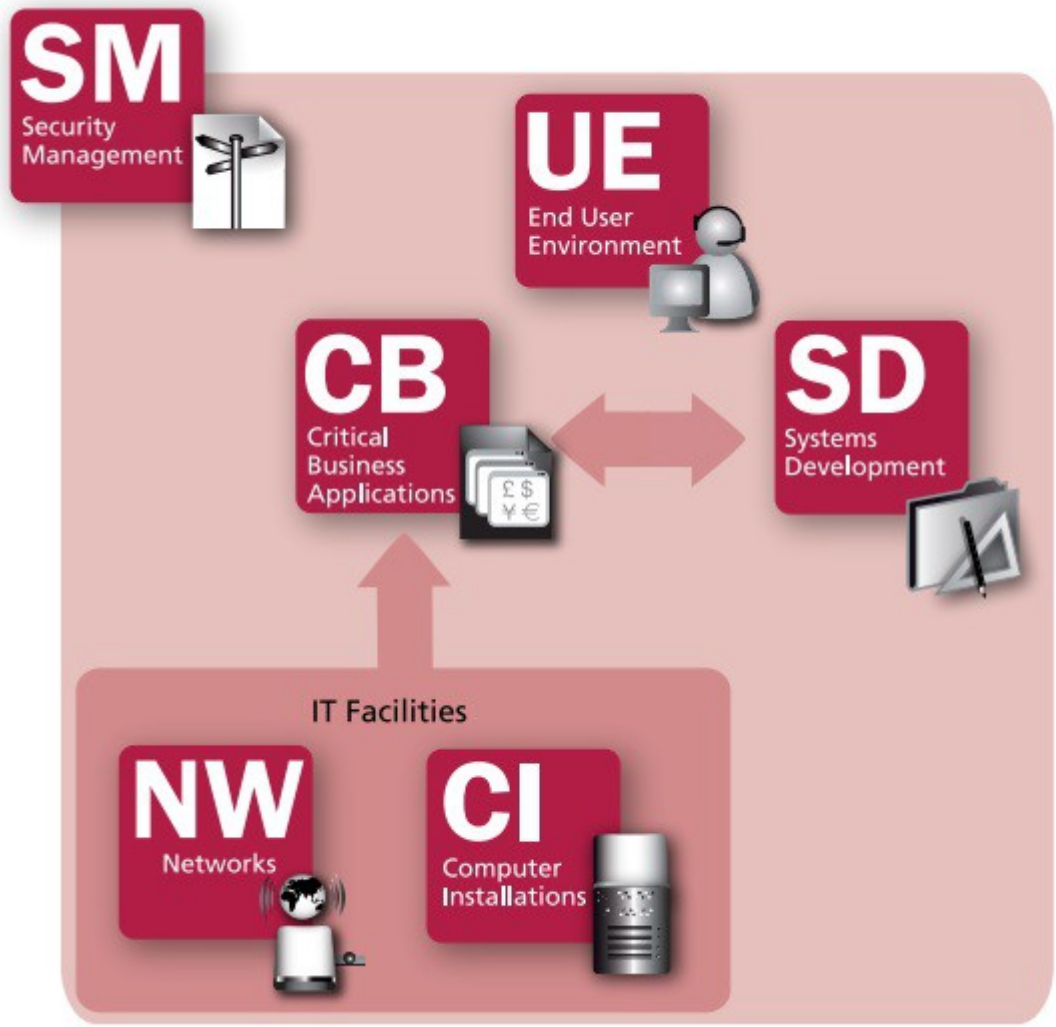
1. Hallinnollinen tietoturva – tietoturvan johtaminen ja hallinnointi
2. Fyysinen tietoturva – toimitilojen ja laitteiden fyysinen suojaaminen
3. Laitteistoturvallisuus – käytettävien laitteiden yleinen suojaaminen
4. Ohjelmistoturvallisuus – käytettävien ohjelmistojen tietoturvallisuus
5. Tietoaineiston turvallisuus – tietoja sisältävien dokumenttien käsittely (sähköiset ja paperiset materiaalit)
6. Tietoliikenneturvallisuus – tiedonsiirtoon liittyvä turvallisuus
7. Henkilöstöturvallisuus – henkilöstön roolit, vastuut ja ohjeistus
8. Käyttöturvallisuus – päivittäisten toimintojen ja rutiinien turvaaminen. (Laakso 2010.)

Tässä työssä pohjana tullaan kuitenkin käyttämään Information Security Forumin The Standard Of Good Practice for Information Security -tietoturvastandardia (tästä eteenpäin SoGP). SoGP:n valinnalla aiheeseen saadaan uusi näkökulma. Kahdeksan osa-aluetta mainittiin tässä työn osassa siksi, että osien jaottelussa ei ole yhtä virallista versiota.

SoGP:ssa tietoturva on jaettu kuuteen osa-alueeseen:

1. Security Management (SM) – Turvallisuusjohtaminen
2. Critical Business Applications (CB) – Yritykselle kriittiset sovellukset
3. Computer Installations (CI) – Laitteet
4. Networks (NW) – Verkot
5. Systems Development (SD) – Järjestelmien kehitys

6. End User Environment (UE) – Loppukäyttäjän ympäristö.



Kuva 2: Tietoturvan osa-alueet SoGP:ssa (ISF 2007, 3).

Kuten kuvasta 2 selviää, laitteet ja verkot muodostavat yhdessä infrastruktuurin, jonka päällä yritykselle kriittiset sovellukset toimivat. Loppukäyttäjän ympäristö vastaa tiedon käsittelyyn ja liikeprosesseihin käyttävien sovellusten turvaamiseksi vaadittavien toimenpiteiden toteutumisesta. Järjestelmien kehitys vastaa siitä, miten uusia sovelluksia ja järjestelmiä tulee kehittää ja tietoturvajohtaminen käsittelee johdon suunnalta tulevaa ohjeistusta sekä valvontaa. (ISF 2007, 3.)

SoGP on lähes 400-sivuinen epävirallinen standardi, joka on jaettu kahteen osaan. Ensimmäinen osa, Principles and Objectives (vapaasti suomennettuna perusperiaatteet ja päämäärät), on tarkoitettu yritysjohdolle, ja tästä osasta löytyy suuntaa antavat tiedot, mitä kukin osuus standardista pitää sisällään ja mitä osuudella tullaan saavuttamaan. Jälkimmäisessä osassa on tarkat selosteet osuuksista, ja tämä osa on tarkoitettu tietoturvahenkilöstön käyttöön. Tämä raportti perustuu lähinnä yritysjohdolle tarkoitettuun osuuteen. Tarpeen mukaan tietoturvahenkilöstölle tarkoitetusta osiosta otetaan huomioon tarkentavia kohtia.

Koska SoGP on tarkoitettu suurten organisaatioiden käyttöön, on osa toimenpiteistä ylimitoitettuja pk-yritysten käytössä. Näiltä osin tässä työssä esiintyviä tietoja tulee soveltaa tapauskohtaisesti niin, että yritykseen sovellettavat toimet ovat verrattavissa mahdollisimman hyvin standardin kanssa. Esimerkkinä voidaan pitää tietoturvapäällikön palkkaamista; pk-yrityksessä voi olla vain yksi työntekijä, tai muutamia työntekijöitä, jolloin tietoturvapäällikön palkkaaminen ei ole taloudellisesti mahdollista. Tällöin yrityksen ainoa työntekijä soveltaa ohjeita omaan työhönsä sopivaksi tai vastuut jaetaan eri työntekijöiden kesken.

SoGP:n viimeisin ilmainen julkaisu on vuodelta 2007, ja uusin maksullinen versio on julkaistu kesäkuussa 2013, ja julkaisun arvo viittaushetkellä 26.6.2014 on 2950 puntaa. Vuoden 2007 standardista puuttuu muun muassa pilvipalveluiden tietoturva. Pilvipalveluiden tietoturvaan liittyvät samat riskit kuin yrityksen omaan tietoturvaan. Huomioon otettavaa on kuitenkin se, että palveluntarjoajat eivät voi omien tietoturvasääntöjensä mukaan kertoa kovinkaan yksityiskohtaisesti siitä, miten ovat hoitaneet osaltaan tietoturva-asiansa. Esimerkiksi palveluun talletetun tiedon fyysinen sijainti vaikuttaa siihen, minkälaista lainsäädäntöä tiedon käsittelyyn sovelletaan.

4.1 Turvallisuusjohtaminen – Security Management (SM)

Yrityksen toimintaan liittyvien tietoturvariskien pitämiseksi hallittuna, tarvitsee yritys korkeimmalta johdolta selkeän suunnan ja sitoutumisen tietoturva-asioi-

den toteuttamiseen. Lisäksi tarvitaan riittävät resurssit ja oikeat järjestelyt, joilla kannustetaan koko yrityksen henkilökuntaa hyvien tietoturvakäytäntöjen toteuttamiseen. Turvallisuusjohtaminen määrittää yrityksessä toimeenpantavan käytännön tietoturvapolitiikan, tietoturvakäytännöt sekä henkilökuntaa sitovan ohjeistuksen. (ISF 2007, SM1.1)

4.1.1 Johtamisjärjestelmät ja hallinnan apuvälineet

Riskienhallinnan ottaminen yritysjohdon johtamisjärjestelmien osaksi hyödyttää yritystä. Riskienhallinnan toimiessa oikein, yrityksen kohdistuvia riskejä saadaan tunnistettua, sekä riskien aiheuttamiin vahinkoihin pystytään varautumaan ennakolta. Tietoturvallisuus on osa yrityksen riskienhallintaa. (Valtiovarainministeriö 2007.)

Tietoturvapolitiikka on yleisluontoinen dokumentti, jonka avulla yritys määrittelee itselleen tavoitteet joihin tietoturvatoiminnalla pyritään. Tietoturvapolitiikassa määritetään myös aiheeseen liittyvät vastuut ja toimintatavat. Dokumentti on yritysjohdon allekirjoittama ja yleensä julkinen asiakirja. (Valtiovarainministeriö 2007, 25.) Tällöin yrityksen sidosryhmille tiedotetaan, että yrityksessä panostetaan tietoturvaan. Tietoturvapolitiikka vaihtelee toimijoittain ja myös julkisia tietoturvapolitiikka-asiakirjoja on lukuisia. Jokainen voi etsiä näitä esimerkiksi internetin hakukoneiden kautta käyttämällä hakusanaa ”tietoturvapolitiikka”.

Jatkuvuus- ja toipumissuunnitelmien avulla taataan yritystoiminnan jatkuvuus mahdollisten poikkeustapausten jälkeen. Suunnitelmien avulla valmistaudutaan poikkeustilanteisiin sekä siihen, että poikkeustapaukset aiheuttavat mahdollisimman vähän vahinkoa yrityksen toimintaan. Jatkuvuussuunnitelma tehdään riskianalyysin perusteella (ISF 2007, SM4.7).

Jatkuvuussuunnitelmassa varaudutaan vakaviin onnettomuuksiin, joita voivat olla esimerkiksi tulipalot, putkirikot, tietoverkkoihin kohdistuvat verkkohyökkäykset ja muut yritystoimintaa haittaavat tapahtumat. Yrityksen toimintaprosessien riippuvuus tietotekniikasta tulee käydä läpi ja kriittisille toiminnoille tulee suunnitella poikkeustilanteiden varalle varajärjestelyt. Varajärjestelyjen, kuten esimer-

kiksi varmuuskopioinnin, toimimisesta tulee varmistua testaamalla järjestelyjen toiminta ennen kuin ne hyväksytään jatkuvuussuunnitelmassa käytettäväksi. (Valtiovarainministeriö 2007, 75-76.)

Toipumissuunnitelma on dokumentti, jossa kuvataan miten yrityksen toiminta saadaan palautettua normaaliksi poikkeustilanteen jälkeen. Kuvauksissa käydään läpi miten varajärjestelyistä siirrytään takaisin järjestelmien normaalikäyttöön. Toipumissuunnitelma tehdään erikseen jokaiselle jatkuvuussuunnitelmassa mainitulle järjestelmälle. (Valtiovarainministeriö 2007, 77.)

4.1.2 Johdon sitoutuminen

Ylimmän johdon tulisi osoittaa sitoutumisensa valitun tietoturvapolitiikan ajamiseen. Sitoutuminen voidaan osoittaa, mikäli yritys haluaa saavuttaa korkean tason hallinnointikoodin saralla, tietoturvaa pidetään yritykselle kriittisenä asiana, yritykseen luodaan tietoturvallisuutta edistävä ilmapiiri ja osoitetaan kolmansille osapuolille, että yritys ottaa tietoturva-asiat ammattimaisella tavalla. (ISF 2007, 84.)

Johdon tulee sitoutua soveltamaan perustavanlaatuisia toimintaperiaatteita yrityksen toiminnassa. Näitä periaatteita ovat, että johto ottaa vastuu yrityksen sisäisestä hallinnoinnista, takaa että yrityksen tietoja ja järjestelmiä hallitaan riskien vaatimalla tavalla, nimittää omistajille vastuun tietojen ja järjestelmien tunnistamisesta, luokittelusta ja turvaamista sekä pääsy tietoon taataan määrättyjen selkeiden ja tarkkojen kriteereiden mukaan. (ISO/IEC 27001:fi 2006, 16; ISF 2007, 84.)

Osoittaakseen sitoutumisensa tietoturva-asioihin, johdon tulisi delegoida vastuut selkeästi tietoturva-asioista vastaavalle henkilölle, esimerkiksi tietoturvapäällikölle. Lisäksi yrityksen tietoturvatilannetta tulee tarkkailla ja huolehtia, että tietoturvan hoitamiseen on varattu tarpeeksi rahaa sekä henkilöresursseja. Allekirjoittamalla tietoturvaa koskevan strategian, toimintatavat sekä koko organisaation laajuisen turvallisuusarkkitehtuurin, on johto osoittanut olevansa sitoutunut yrityksen tietoturva-asioihin. (ISO/IEC 27001:fi 2006, 16; ISF 2007, 84.)

4.1.3 Suojattavat kohteet ja kohteiden luokitus

Kohteiden suojausta suunnitellessa tulee ottaa huomioon suojattavien kohteiden sekä käytettävien suojakeinojen hinta. Suojaus voi maksaa joko rahallisesti liikaa, tai sitten suojaus voi aiheuttaa järjestelmien suorituskyvyn heikkenemistä siinä määrin, että suojauksesta saatava hyöty on pienempi kuin menetetty suorituskyky tai suojauksen aiheuttama haitta. (Andress 2011, 22.) Suojaus tehdään ottamalla huomioon CIA-kolmion ominaisuudet.

Suojattavat kohteet eivät ole aina fyysisiä kohteita. Esimerkiksi yrityksen imago ja tuotemerkit voivat menettää arvoaan tietoturvarikkeiden vuoksi. Vuonna 2011 Sonyn PlayStation Network joutui ulkopuolisen hyökkäyksen kohteeksi. Hyökkäys esti tai vaikeutti 77 miljoonaa asiakasta käyttämästä verkkoa usean päivän ajan. Sony menetti tapauksen vuoksi 171 miljoonaa dollaria (Hachman 2011). Rahallisen menetyksen lisäksi yhtiö kärsi ison imagotappion. Isot monikansalliset yhtiöt voivat korjata tahriintunutta imagoaan mainoskampanjoilla, mutta pienyrityksen maineen menetys voi johtaa pahimmillaan liiketoiminnan loppumiseen.

Jotta yrityksessä oleva tieto suojataan sille sopivalla tavalla, tulee tiedon arvo yritykselle määritellä ja luokitella arvon mukaan. Arvo voidaan määrittää esimerkiksi sen mukaan, minkä verran vahinkoa tiedon luottamuksellisuuden menettäminen aiheuttaisi yrityksen toiminalle. Tämän jälkeen tieto luokitellaan asteikolla, jonka toisessa päässä ovat julkiset tiedot, ja toisessa päässä ovat yrityksen toiminalle kriittiset tiedot. Luokitteluohjeisiin määritellään yrityksen tarpeisiin sopiva määrä turvaluokkia. (ISF 2007, SM3.1; Valtiovarainministeriö 2010.). Pienellä yrityksellä luokat voivat olla julkinen, luottamuksellinen ja salattu. Määrityksen tulee ottaa huomioon paperidokumentit, sähköisessä muodossa olevat dokumentit sekä sähköinen kommunikointi (esimerkiksi sähköposti ja pikaviestimet). (ISF 2007, 95; ISO/IEC 27001:fi 2006.)

Luokittelumäärittelyn jälkeen jokaiselle luokalle määritellään tiedon käsittelyyn, säilytykseen ja siirtoon liittyviä ohjeita. Esimerkiksi luottamukselliset tiedot ovat yrityksen henkilökunnan käytössä ohjeistuksen sallimissa rajoissa, ja salatut tie-

dot vain määrättyjen henkilöiden käytössä. Käyttöoikeuksien lisäksi tiedon siirtoa voidaan rajoittaa. Tiedon siirto yrityksen tiloista voidaan kieltää, ellei tietoa ole salattu. Tietojen luokittelu ei koske pelkästään dokumentteja, vaan dokumenttien käsittelyyn sekä tietojen siirtoon käytettävät laitteet suojataan luokittelun vaatimalla tavalla (ISF 2007, SM3.1.).

Kun tieto on suojattu luokituksen vaatimalla tavalla, tulee luokituksen paikkansa pitäminen tarkastaa määrätyin väliajoin. Luokitukseen liittyvän ohjeistuksen tulee neuvoa miten materiaalia käsitellään kun materiaalia kopioidaan, säilytetään tai tuhotaan. (ISF 2007, SM3.1.3-SM3.1.4.) Luokitellusta materiaalista tulee pitää kirjaa, josta selviää salatun tiedon luokka, tiedon omistaja sekä lyhyt tiivistelmä tiedon sisällöstä. (ISF 2007, SM3.1.8)

4.1.4 Omistajuus

Kaikelle suojaluokituksen saaneelle tiedolle sekä kriittisille järjestelmille tulee määrätä omistaja. Omistaja on vastuussa muun muassa siitä, että tieto, tai järjestelmät, ovat suojattu niiden vaatimalla tavalla. Hän vastaa myös siitä, että tietoa tai järjestelmiä pääsevät käsittelemään vain ne henkilöt, joilla on siihen oikeus. Mikäli omistajuuden vaihtaminen on tarpeen, uuden omistajan määrääminen on vanhan omistajan vastuulla. (ISF 2007, SM3.2)

ISO/IEC 27001:fi 2006 määrittelee omistajan seuraavasti: ”Termillä ”omistaja” yksilöidään henkilö tai yksikkö, jolla on hyväksytty esimiesvastuu suojattavien kohteiden tuottamisen, kehittämisen yläpidon, käytön ja turvallisuuden valvonnasta. Termi ”omistaja” ei tarkoita, että kyseisellä henkilöllä olisi minkäänlaisia omistajuusoikeuksia”. (ISO/IEC 27001:fi 2006, 17.) Omistajuuden avulla saadaan vastuuta delegoitua pois ylimmältä johdolta. Yrityksen omistaja, tai ylin johtaja, on kuitenkin aina lopulta vastuussa yrityksen tietoturva-asioiden toimimisesta (BSI 2014, 7).

4.1.5 Tietoturvakäytännöt ja -periaatteet sekä ohjeistus

Tietoturvakäytännöt ja -periaatteet on dokumentti, jossa kuvataan käytännön ratkaisut, joiden avulla yrityksen tietoturvaa normaalisti hallitaan. Dokumenttia voidaan kutsua eri lähteissä myös tietoturvasuunnitelmaksi. Tähän dokumenttiin kirjataan esimerkiksi yrityksen käytössä olevat tietoturvaratkaisut, minkälaisia tietoturvatoimenpiteitä tulevissa kehittämishankkeissa käytetään ja tietoaineiston käsittelyyn, sekä tietoturvatoiminnan tulosten raportointiin liittyviä asioita. (Valtiovarainministeriö 2007.)

Kun yrityksen johto on sitoutunut toimimaan yrityksen tietoturvan kehittämiseksi, tulee yrityksessä tuottaa yksityiskohtainen, dokumentoitu ja päivitettävä tietoturvaohjeistus. Tämä ohjeistus tulee saattaa jokaisen sellaisen henkilön tietoon, jolla on pääsy yrityksen tietoihin tai järjestelmiin. Dokumentteihin kirjataan henkilöiden vastuut, sekä tietoturvaperiaatteet, joita koko henkilökunnan tulee noudattaa. (ISF 2007, SM1.2; ISO/IEC 27001:fi 2006, 18.)

Tietoturvaohjeistus tulee olla linjassa muiden yrityksessä käytössä olevien korkean tason käytäntöjen, kuten tietoturvakäytäntöjen ja -periaatteiden, kanssa. Nämä käytännöt liittyvät muun muassa henkilöstöhallintoon, työntekijöiden terveyteen ja turvallisuuteen, rahoitukseen ja tietotekniikkaan. Ohjeistus tulee käydä läpi säännöllisesti täsmällisen arvosteluprosessin avulla ja päivittää olosuhteiden muuttuessa. Olosuhteiden muutoksia voivat olla esimerkiksi uusien uhkien ilmaantuminen, haavoittuvuudet, organisaatiomuutokset, sopimusten muutokset, lainsäädännön tai määräysten muutokset sekä IT-infrastruktuurin muutokset. (ISF 2007, SM1.2.)

Tietoturvaohjeistuksen tehokkuutta voidaan tukea saattamalla henkilökunta tietoiseksi siitä, että ohjeistuksen noudattamatta jättäminen voi aiheuttaa kurinpidollisia toimia. (ISF 2007, SM1.2; Andreasson ym. 2013, 86.)

Tietoturvaohjeistuksen tulee vaatia seuraavia asioita:

- puhtaan pöydän politiikan noudattamista

- sähköpostin turvallista käyttämistä
- kirjautumaan ulos työasemilta, mikäli työpisteeltä poistutaan. (ISF 2007, SM1.2; ISF 2007 SM6.3.)

Tietoturvaohjeistuksen pitää ehdottomasti kieltää seuraavat asiat:

- yrityksen tietojen ja järjestelmien luvaton käyttö
- yritysten tietojen ja järjestelmien käyttö muuhun kuin työhön liittyviin asioihin
- epäasiallinen ja laiton käytös
- laittoman materiaalin lataaminen
- yrityksen materiaalin vieminen pois työpaikalta
- ulkopuolisten muistilaitteiden käyttö (esimerkiksi USB-tikut, kolmansien osapuolten ohjelmistot, modeemit)
- yrityksen ohjelmistojen luvaton kopioiminen
- salasanojen kirjoittaminen muistiin (esimerkiksi muistilapulle tai matkapuhelimen muistiin)
- sellaisen tiedon käyttö, josta voi selvitä jonkun henkilön identiteetti, paitsi mikäli tällaisen tiedon käyttöön on annettu lupa
- työasioihin liittyvien asioiden keskustelu julkisilla paikoilla. (ISF 2007, SM1.2.)

4.1.6 Henkilökunnan sitouttaminen, koulutus ja propaganda

Työhönottotilanteessa työntekijän taustatiedot, mukaan lukien koulutukseen liittyvät tiedot, tarkastetaan. Tietoturvaan liittyvät vastuut ja velvoitteet tulee ilmetä sopimuksissa, ja ottaa huomioon henkilöitä palkattaessa. Kun tietoturva-asiat kuuluvat työvelvoitteisiin, saadaan henkilökunta työskentelemään tietoturvaohjeiden mukaisesti. Nämä velvoitteet ovat voimassa myös työajan ulkopuolella sekä työsuhteen päättymisen jälkeen. (ISF 2007, SM1.3.)

Työntekijöille tulee pitää koulutusta, jossa heille opetetaan tietoturvaan liittyviä asioita. Koulutuksen tavoitteena on se, että henkilökunta osaa arvioida turvalli-

suusvaatimuksia. Tällöin he osaavat tarpeen mukaan ehdottaa uusia kontrolleja, ehdottaa korjauksia käytössä oleviin toimimattomiin kontrolleihin sekä toimeenpanna uusia kontrolleja. (ISF 2007, SM2.5; Andreasson ym. 2014, 58.) Järjestelmien väärän käytön aiheuttamat haitat saadaan minimoitua, kun työntekijöille opetetaan järjestelmien oikeat käyttötavat. Henkilökunnan osaamisesta voidaan varmistua järjestämällä heille määräajoin tietoturvaosaamista kartoittavia testejä. Testin tulosten perusteella voidaan korjata mahdolliset löydetyt epäkohdat, olivatpa ne ohjeistuksesta tai henkilökunnan osaamisesta johtuvia. (Andreasson ym., 2014; ISO/IEC 27001:fi 2006, 18.)

Yrityksen riippuvuus yrityksen toimintaan liittyvistä avainhenkilöistä tulee tiedostaa. Yritys voi sitouttaa henkilökuntaansa palkitsemisjärjestelyin tai varmistamalla, että työviihtyvyys ja motivaatio ovat kunnossa. (Valtiovarainministeriö 2007, 57.) Varsinkin pienyrityksissä voi aiheutua ongelmia siitä, että avainhenkilön osaaminen ei ole syystä tai toisesta käytettävissä.

4.1.7 Asiakkuuden ja työsuhteen päättäminen

Asiakassuhteen päättymiseen liittyvät käytännöt tulee selvittää. Asiakkaalla voi olla pääsy yrityksen järjestelmiin tai yrityksellä on hallussaan asiakkaalle kuuluvaa tietoa. Asiakassuhteen päättymisen jälkeen tulee varmistaa että asiakkaan käyttöoikeudet on peruttu, eikä lain määräämän tiedon lisäksi muuta asiakkaaseen liittyvää tietoa löydy yrityksen järjestelmistä.

Yrityksen on suositeltavaa kirjata ylös toimintaperiaatteet palvelusopimuksiin liittyvien käytäntöjen osalta, mikäli yrityksellä on tarve käyttää palveluntarjoajia. Esimerkiksi palvelusuhteen aloitukseen ja lopetukseen liittyvät toimenpiteet ovat huomioitavia asioita.

Työntekijöillä on työsuhteen aikana pääsy yrityksen järjestelmiin sekä tietoihin. Työsuhteen päättymisen jälkeen pitää varmistua että työntekijän käyttöoikeudet järjestelmiin poistetaan sekä yrityksen omaisuus palautetaan. (ISO/IEC 17799:fi 2006, 33-34.)

4.1.8 Tietotilinpäätös

Tietotilinpäätös on raportti, joka käsittelee yrityksen tietovarantoja, tietojohtamista, tietojenkäsittelyä ja tietoturvallisuutta. Tietotilinpäätös voidaan pitää yrityksen sisäisenä raporttina, jolloin se ohjaa henkilökuntaa hyvään tietojenkäsittelytapaan. Tietotilinpäätös voidaan suunnata myös yrityksen sidosryhmille, jolloin raportti antaa tietoa yrityksen tavasta käsitellä tietovarantojaan. (Tietosuojavaltuutetun toimisto 2012; Andreasson ym. 2014, 119.)

Tietosuojavaltuutetun toimiston julkaisema Laadi tietotilinpäätös -oppaasta selviää, että tietotilinpäätös muun muassa:

- kertoo minkälaisessa tilassa organisaation tietojenkäsittely on
- kertoo mitä tietovarantoja organisaatio omaa
- kuvaa organisaation toimintaan liittyvää tietoturvan ja -suojan toteuttamista
- kuvaa miten yrityksessä toteutetaan tietojenkäsittelyyn liittyvä riskienhallintaa
- tukee organisaatiossa tapahtuvaa suunnittelun ja toiminnan ohjausta
- varmistaa, että organisaatiossa noudatetaan sen toimitaan liittyvää lainsäädäntöä. (Tietosuojavaltuutetun toimisto 2012; Andreasson ym. 2014, 118.)

Sisältämänsä informaation vuoksi tietotilinpäätös on hyvä yritysjohdon työväline. Hyvin tuotetusta tietotilinpäätöksestä selviää yrityksen, sekä asiakkaiden, välillä olevat tiedolliset tarpeet. Samalla yritysjohdon kuva yrityksen tietoturvaan liittyvistä asioista selkeytyy. (Tietosuojavaltuutetun toimisto 2012.)

4.2 Kriittiset sovellukset – Critical Business Applications (CB)

Kriittiset sovellukset ovat sovelluksia, jotka ovat välttämättömiä yrityksen toiminnan kannalta. Näihin sovelluksiin käytetään tiukempia kontrolleja kuin tavallisiin sovelluksiin, koska sovelluksissa käsitellään yritykselle tärkeää tietoa. Kriittisen

tiedon luottamuksellisuuden, eheyden tai saatavuuden menettäminen aiheuttama haitta on yritykselle suurin. (ISF 2007.)

Kriittisten sovellusten käyttäminen, ja pääsy sovellusten käyttämään tietoon, tulee rajata vain tarpeellisille henkilöille. Myös kirjautumisista tulisi pitää kirjaa. Kyseisten henkilöiden käyttöoikeudet tulee rajata niin, että heillä on käytössään mahdollisimman vähän käyttöoikeuksia. Käyttöoikeudet tulevat rajat käyttäjän työroolin mukaan. Käyttöoikeudet tulee poistaa heti kun käyttäjä ei niitä enää tarvitse. (ISF 2007, CB3.1.)

4.2.1 Kontrollit

Yritykselle kriittistä tietoa käsittelevät sovellukset, sekä sovelluksia käyttävät järjestelmät, tulee suojata tiukemmin kuin vastaavat normaalikäytössä olevat sovellukset ja järjestelmät. Sovelluksiin tehtävistä syötteistä tulee varmistaa, etteivät ne sisällä vääriä tai sopimattomia arvoja. Eri järjestelyjen avulla tulee varmistua, että tietoa ei voi ylikirjoittaa vahingossa ja ettei tietoon voi tehdä huomaamattomia muutoksia. (ISF 2007, CB2.2)

Kriittisen tiedon käsittelemiseen käytettävät käyttöjärjestelmät tulee kovettaa, eli käyttöjärjestelmien tarpeettomat osat tulee ottaa pois käytöstä ja turhat käyttäjätilit tulee sulkea. Laitteissa käytettävät oletussalasanat tulee vaihtaa. Mikäli on tarpeellista, lokienhallinnan avulla voidaan tarkkailla järjestelmän vakautta, sisäänkirjautumisia ja mahdollisia aiheettomia käyttöoikeuksien muutosyrityksiä. (ISF 2007, CB2.2)

4.2.2 Arkaluontoisen materiaalin suojaaminen ja hävittäminen

Arkaluontoisen materiaalin käsittely aiheuttaa lisätoimia. Tällöin varmistutaan, ettei materiaali joudu vääriin käsiin tai ettei tiedon eheys vaarannu. Mikäli tietoa siirretään sovellusten tai kolmansien osapuolten välillä, voidaan tieto suojata salaustekniikkaa käyttämällä. Tällöin tiedon luottamuksellisuudesta on varmistuttu. Lisäksi tiedon muuttumattomuudesta ja kiistämättömyydestä on huolehdittu.

Mikäli yritys joutuu säilyttämään arkaluontoista materiaalia fyysisessä muodossa, tulee materiaali säilyttää paloturvallisessa lukitussa kaapissa. Kun materiaalia siirretään paikasta toiseen, tulee materiaalia käsittelevät henkilöt kirjata ylös, sekä merkitä materiaali tunnistettavalla tavalla. Hävittämällä materiaali käytön jälkeen turvallisesti, esimerkiksi silppurissa, estetään materiaalin päätyminen ulkopuolisten käsiin. (ISF 2007, CB2.6.)

Vaikka tiedot poistetaan tavallisesti esimerkiksi kovalevyltä tai muistitikulta, tieto ei ole vielä kadonnut pysyvästi tallennusmediasta. Tieto on helposti palautettavissa luettavaan muotoon. Jotta tieto poistuu lopullisesti talletusmedialta, täytyy sen ylle kirjoittaa uutta tietoa. Poistettaessa käytöstä tietokonelaitteita, tai esimerkiksi tulostimia, asianmukaisen hävitysprosessin avulla estetään tiedon päätyminen ulkopuolisille. Paperimateriaalin ja optisten levyjen tuhoaminen on helpompaa. Paperin silppuaminen tai levyn tuhoaminen estävät tiedon lukemisen. (Andress 2011, 107.)

4.2.3 Ulkopuoliset yhteydet

On mahdollista, että kriittiseen sovellukseen joudutaan olemaan yhteydestä yrityksen verkon ulkopuolelta. Yhteyden avaamisen tarvitaan aina prosessista vastaavan henkilön lupa ja kaikista yhteyksistä tulee pitää kirjaa. Tarpeen mukaan pääsy sovellukseen voidaan estää palomuurien tai välityspalvelinten avulla. (ISF 2007, CB4.3.)

4.2.4 Varmuuskopiointi

Keskeisten tietojen ja ohjelmien varmuuskopioinnista tulee huolehtia. Varmuuskopioinnissa tulee käyttää varmuuskopioinnin hallintaan sopivia järjestelyjä. Varmuuskopioinnin hallinnalla varmistetaan, että tiedot ovat suojattu ulkopuolisilta, sekä oikeat tiedot saadaan ongelmatapauksissa nopeasti takaisin yrityksen käyttöön. Tietojen luottamuksellisuus ja eheys saavutetaan salauksella ja tarkastussummien käytöllä.

Varmuuskopioista on hyvä säilyttää kopio muualla kuin yrityksen tiloissa. Tällöin esimerkiksi tulipalon vuoksi ei menetetä kaikkia varmuuskopioita. Fyysiset tallennusvälineet tulee merkitä päiväyksin, sekä selostein jossa selvitetään mitä tallennusväline sisältää. Varmuuskopioinnin palautuksia on hyvä harjoitella, jotta palautusprosessiin mahdollisesti liittyvät ongelmat saadaan karsittua. (ISF 2007, CB4.4; Andress 2011, 107-108.)

4.3 Laitteet – Computer Installations (CI)

CI-osa-alueen tarkoituksena on selvittää miten tarpeet tietokonejärjestelmille on tunnistettu, miten tietokoneet tulee asentaa ja miten niitä käytetään, jotta tarpeet tulevat täytetyiksi. Tämä osa-alue tutkii kaiken kokoisia tietokonejärjestelmiä, isoista keskustietokoneista yksittäisiin tietokoneisiin. Järjestelmät voivat olla yleisessä työkäytössä, tai ne voivat olla tarkoitusta varten rakennettuja konesaleja, joissa on käytössä käyttöjärjestelmä, esimerkiksi Windows 7 tai Unixin kaltainen käyttöjärjestelmä. (ISF 2007.)

4.3.1 Laitteiden ja järjestelmien fyysinen suojaaminen

Tietokoneisiin kohdistuu monenlaisia uhkia, ulkopuolisten tahojen verkkohyökkäyksistä työntekijöiden haitantekoon. Suojaamalla järjestelmät ja laitteet saadaan kyseisiä uhkia pienennettyä. Yrityksessä tulee varautua laiterikkoihin ja käyttöön liittyviin ongelmiin etukäteen dokumentoimalla toimintaohjeet siitä, miten henkilökunnan tulee toimia laiterikkojen tapahtuessa. Ohjeissa voidaan kertoa yleisimmät vikatilanteet ratkaisuehdotuksineen. (ISF 2007, CI3.5)

Tarkkailemalla toimintaympäristön olosuhteita ja pitämällä ne asianmukaisina, laitteiden toimintaan liittyvät riskit minimoidaan. Ihmisten toimien jälkeen tuleen, veteen, likaan ja sähköön liittyvät asiat aiheuttavat suuren osan laitteisiin kohdistuvista uhista. Palohälytyslaitteistolla, ja oikein sijoitetuilla ensisammutusvälineistöllä (ISO/IEC 17799:fi 2006, 100; ISF 2007, CI2.6), saadaan torjuttua alkavia tulipaloja. Kun tulta torjutaan vedellä, pitää huomioida että vesi itsessään ai-

heuttaa vaaran laitteille (Andress 2011, 110). Veteen liittyviä uhkia voidaan torjua viemäröinnillä ja kaksoislattioiden avulla. Virransyöttöön liittyviä ongelmia voidaan ratkaista esimerkiksi keskeytymättömän sähkönsaannin varmistavilla UPS-laitteilla sekä vikavirta- ja ylijännitesuojilla (ISF 2007, CI2.7). Pölyä vastaan voidaan suojautua huoltamalla laitteita määräajoin. (ISO/IEC 17799:fi 2006, 37-38.)

Laitteisiin liittyviä riskejä voidaan ehkäistä rajoittamalla asiattomien henkilöiden fyysinen pääsy laitteille. Jokaisen henkilökunnan jäsenen ei tarvitse päästä käyttämään jokaista yrityksen laitetta. Laitteiden sijoittaminen niin, etteivät ne ole suoraan näkyvillä, tai pitämällä ne lukituissa kaapeissa, vähennetään laitteisiin kohdistuvia väärinkäytöksiä. Laitteet voidaan kiinnittää työpöytiin vaijerein, jolloin niiden vieminen yrityksen tiloista estetään. Kun laitteet on merkitty pysyvillä tunnistemerkinnöillä, varastetun tavaran takaisin saaminen helpottuu. (ISO/IEC 17799:fi 2006; ISF 2007, CI2.8; Andress 2011, 110-111.)

4.3.2 Laitteiden käyttöön liittyvä suojaaminen

Laitteet tulee kovettaa, eli rajoittaa käytössä olevien toimintojen määrää. Poistamalla ohjelmia tai rajoittamalla käyttöjärjestelmän osien toiminnallisuuksia, saadaan järjestelmien hyökkäyspinta-alaa pienennettyä. Mikäli työntekijöillä on oikeudet muuttaa järjestelmien asetuksia, olkoon muutos vahinko tai tahallaan tehty, voivat muutokset estää järjestelmien toiminnan. Tästä syystä asetusten muuttaminen pitää estää työntekijöiltä ja jättää asiantuntijoiden tehtäväksi. Lisäksi laitteet ja järjestelmät tulee varustaa haittaohjelmien ja virusten torjuntaan soveltuvilla ohjelmilla sekä internetyhteydessä olevat järjestelmät palomuuriohjelmistoilla. (ISF 2007, CI2.3-CI2.4; Andress 2011, 134.)

Järjestelmien kautta on pääsy lähes kaikkeen yrityksen käytössä olevaan tietoon. Siksi onkin tärkeää, että laiteet suojataan fyysisen pääsyn lisäksi sisäänkirjautumiseen liittyvillä suojakeinoilla. Sisäänkirjautumisen, käyttäjien tunnistamisen ja käyttöoikeuksien myöntämisen suhteen tulee määritellä toimintatavat. Eräs tapa on toimia pienimmän oikeuden periaatteella; käyttäjälle annetaan vain

sen verran käyttöoikeuksia jotta työprosessi saadaan suoritettua. (ISF 2007 CI; Andress 2011, 34.)

4.4 Verkot – Networks (NW)

Yrityksen sisäiset verkot välittävät tietoa ja sallivat yhteydet eri tietojärjestelmien välillä. Verkot ovat ominaisuuksiensa vuoksi alttiita häiriöille, joten hyvin suunnitellut ja hoidetut verkkoyhteydet takaavat toimintaprosessien sujuvuuden. Tietoliikenneverkkojen lisäksi puhelinverkot ovat alttiina uhille. (ISF 2007.)

4.4.1 Suunnittelu, konfigurointi ja dokumentointi

Hyvin suunniteltu verkko estää osan verkkoihin kohdistuvista uhista. Hyvä suunnittelu lieventää osaa uhista ja hyökkääjien tunkeuduttua verkkoon vähentää mahdollisuuksia aiheuttaa tuhoa. Verkko tulee jakaa fyysisesti tai loogisesti eri osiin eri käyttötarpeiden mukaan. Eri osat eristää niin, että verkkojen välinen liikenne ei ole yhteydessä toisten osien välillä. Liikenne voidaan ohjata esimerkiksi reitittimen ja/tai palomuurin läpi. Verkkoliikenteen valvonta helpottuu, kun ulkoverkosta sisäverkkoon tuleva liikenne päästetään mahdollisimman harvasta solmukohdan läpi. (ISF 2007, NW1.2; Andress 2011, 116.)

Verkkolaitteiden konfigurointi on tärkeä osa verkon rakentamista. Oikein konfiguroidut laitteet lisäävät verkon turvallisuutta. Verkko voidaan asettaa toimimaan niin, että kaikki liikenne on kielletty, ellei liikennettä erikseen sallita. Reitittimien asetuksiin tulee kiinnittää huomiota ja turhat toiminnot tulee kytkeä pois käytöstä. (ISF 2007, NV2.1.) Tällöin verkkoon kohdistuvia uhkia saadaan pienennettyä huomattavasti.

Langattomia yhteyksiä käytettäessä tulee ottaa huomioon tukiasemien kantavuus, salaukseen käytettävät menetelmät ja käyttöoikeudet. Koska langattomien tukiasemien käyttöön liittyy useita tietoturvariskejä, tulee varmistaa että verkkoon ei pysty liittämään omatoimisesti tukiasemia tai muita laitteita. (Andress 2011, 123.)

Verkon dokumentointi auttaa verkon ylläpidossa. Dokumenttien avulla saadaan selkeä kuva, minkälaisista osista verkko koostuu. Dokumentteihin kirjataan verkon infrastruktuuriin käytetyt laitteet, ohjelmistot sekä työasemat ja muut laitteet, jotka verkkoon on kytketty. (ISF 2007, NW1.4)

4.4.2 Sisä- ja ulkoverkon välinen liikenne

Kaikki sisäverkkoon tuleva liikenne pitää reitittää kulkemaan palomuurin läpi. Sama koskee ulospäin suuntautuvaa liikennettä. Tällöin sisäverkossa liikkuva tieto ei ole nähtävissä verkon ulkopuolella. Palomuurien avulla liikenteeseen liittyvät osoitteet, protokollat ja muut tiedot voidaan tarkastaa ja päästää vain haluttu liikenne palomuurin läpi. (ISF 2007, NW2.2)

Välityspalvelinten avulla voidaan tarjota verkon käyttäjille lisäturvaa. Välityspalvelimelle ladataan käyttäjien tarvitsema sisältö, esimerkiksi sähköposti- ja selainliikenne, suodatetaan datapaketit määritettyjen sääntöjen mukaan ja lopuksi välitetään tiedot käyttäjien koneille. Välityspalvelinten avulla saadaan verkkoliikenteestä suodatettua epätoivottua materiaalia pois. (Andress 2011, 119.)

Jos yrityksellä on tarve siirtää arkaluontoista tietoa oman verkon ulkopuolelle, VPN-yhteys (virtual private network) takaa tiedon salassa pysymisen. VPN-ohjelma toimii kahden tai useamman pisteen välillä salaamalla pisteiden välillä kulkevan liikenteen. Tällöin pisteiden välillä kulkeva liikenne pysyy salaisena, vaikka se kulkee esimerkiksi internetin yli. VPN-yhteyksiä voidaan käyttää myös sisäverkon eri osien välillä. (Andress 2011, 122.)

4.4.3 Verkon ulkopuoliset yhteydet ja etäylläpito

Asiakassuhteen hoitaminen voi aiheuttaa tilanteen, jossa yrityksen asiakkaiden on päästävä käyttämään yrityksen verkossa olevia palveluita. Verkko tulee konfiguroida niin, että ulkopuolelta yhteyden ottanut taho näkee yrityksen verkosta vain välttämättömät tiedot. Kaikista yhteyksistä tulee pitää kirjaa. Yhteydenottoon käytettäviä laitteita voidaan rajoittaa esimerkiksi niin, että mobiililaitteilla

yhteyttä ei voi muodostaa. Tarpeettomat yhteydet on suljettava kun niiden käyttöön ei ole enää tarvetta. (ISF 2007, NW2.3.)

Verkon etähuoltoa koskien tulee huolehtia, että vain osaavilla henkilöillä on oikeus suorittaa huoltoja. Huoltajien käyttöoikeuksista tulee huolehtia niin, että oikeudet eivät ole liian suuret. Tallentamalla lokeihin huoltotoimenpiteet ja tarkastamalla lokit jälkikäteen, voidaan varmistua, että toimet ovat olleet huoltotapaukseen sopivia. (ISF 2007, NW3.7.)

4.4.4 Verkon suojaaminen ja valvonta

Verkon kriittisyyden vuoksi verkon suojaamiseen on kiinnitettävä erityistä huomiota. Fyysinen pääsy verkkolaitteille pääsy tulee rajoittaa minimiin. Rajoitus koskee niin yrityksen omaa henkilökuntaa, yhteistyötahoja kuin täysin ulkopuolisia henkilöitä. Verkkolaitteet suojataan samoja uhkia vastaan kuin on käyty läpi tämän raportin kohdassa 4.3.1 Laitteiden ja järjestelmien fyysinen suojaaminen. Verkkolaitteet tulee lisäksi sulkea lukittaviin tiloihin tai kaappeihin. Verkkokaapelit tulee asentaa suojattuihin kaapelikanaviin niin, että kaapelit eivät ole näkyvissä. (ISF 2007, NW3.5.) Varmuuskopioimalla verkon toimintaan liittyvien laitteiden asennustiedostot, saadaan ongelmatapauksissa toimivat asetukset nopeasti käyttöön.

Verkkoa valvomalla on mahdollista reagoida etukäteen verkkoon kohdistuvien uhkien varalta. Mahdollisten väärinkäytösten jälkeen tapausten selvittämistä voidaan helpottaa verkon valvonnan avulla. Verkon valvontaan voidaan käyttää automatisoituja ohjelmistoja, tai vaihtoehtoisesti käydään läpi verkkoliikenteeseen liittyviä lokitiedostoja. Verkon valvonnan avulla voidaan myös tarkkailla verkkoon liitettyjä laitteita ja laitteiden tietoturvan tilaa. (ISF 2007, NW3.1.)

4.5 Järjestelmien kehitys – Systems Development (SD)

Turvallisuuden lisääminen järjestelmiin on huomattavasti kustannustehokkaampaa järjestelmien kehityksen aikana kuin järjestelmän käyttöönoton jälkeen

(ISO/IEC 17799:fi 2006, 75). Tietoturvallisuuden huomioon ottaminen järjestelmien kehityksen jokaisessa vaiheessa on kriittistä järjestelmien turvallisuuden kannalta. Järjestelmillä ei tarkoiteta pelkästään tietokoneissa käytettäviä ohjelmistoja, vaan kaikkia laitteita ja ohjelmistoja, joita liikeprosessien suorittamiseen tarvitaan.

4.5.1 Järjestelmien suunnittelu, kontrollit sekä laadun varmistaminen

Järjestelmien kehittämiseen tulee käyttää dokumentoituja menetelmiä, järjestelmien kehityksen elinkaari -mallia, eli SDLC-mallia mukaillen. Kehityksessä tulee ottaa huomioon yrityksessä käytössä olevat tietoturvakäytännöt, yritystoiminnan vaatimukset sekä lainsäädännön määräämät velvoitteet. (ISF 2007, SD1.2; ISF 2007, SD3.1.) Jos yrityksen käytössä on suunnitellun järjestelmän lisäksi muita järjestelmiä, pitää uuden järjestelmän suunnittelussa ottaa huomioon vanhojen järjestelmien ominaisuudet (ISF 2007, SD4.1).

Kehityksen aikana tulee kartoittaa kehitykseen liittyviä riskejä. Kartoitusta tehtäessä huomioidaan tiedon luottamuksellisuus, eheys ja saatavuus. (ISF 2007, SD.) Turvallisuuteen liittyvät toiminnot tulee tarkastaa kehitysprosessin alkuvaiheessa, sekä sovittujen virstanpylväiden kohdalla. Järjestelmien turvallisuus saadaan turvattua, kun suunnitelmia ja resursseja verrataan ja päivitetään kehitykseen liittyvien muutosten mukana. Mikäli turvallisuuteen liittyviä epäkohtia havaitaan, pitää kehitys keskeyttää ja epäkohdat korjata. (ISF 2007, SD1.2.)

Järjestelmiin liittyviä kontrolleja tulee harkita suunnittelun aikana. Oikein valituilla kontrolleilla voidaan estää esimerkiksi väärien syötteiden käyttö, kriittisen tiedon poistaminen ja ylikirjoittaminen tai tiedon muuttaminen ilman valtuutta. (ISO/IEC 17799:fi 2006, 76; ISF 2007, SD4.3).

4.5.2 Järjestelmien rakentaminen ja hankinnat

Kaikkia järjestelmien osia ei pystytä, eikä tule toteuttaa yrityksen sisäisesti. Tällöin laitteiston asentaminen, tai ohjelmistojen asentamiseen, voidaan käyttää ul-

kopuolisen tahon palveluita. Laitteita, ohjelmistoja sekä palveluita hankittaessa tulee ottaa huomioon hankittavan kohteen käytettävyys, luotettavuus, tietoturva sekä palveluntuottajan asiantuntemus. Käyttämällä hyväksi havaittuja menetelmiä sekä asiantuntevaa henkilöstöä, varmistetaan järjestelmien asianmukaisen rakentaminen. Muutoksiin liittyvät yksityiskohdat on kirjattava ylös, mikäli hankittavaan tuotteeseen on tehty alkuperäisestä versiosta eroavia muutoksia. (ISO/IEC 17799:fi 2006, 75; ISF 2007, SD.)

Mikäli sovelluksella on yhteys internetiin, järjestelmään turvallisuutta parannetaan lisäämällä sovellukseen tietoturvaa parantavia kontrolleja. Kontrolleja suunnitellessa tulee ottaa huomioon raportin kohdassa 4.4 Verkot – Networks (NW) käytyjä asioita.

4.5.3 Testaaminen ja käyttöönotto

Kehityksen alla olevaan järjestelmään liittyy tietoturvariskejä. Yrityksen toiminta ei vaarannu ongelmatapauksissa, kun järjestelmää testataan irrallaan päivittäisestä käyttöympäristöstä. (ISF 2007, SD3.5.) Testauksessa varmistetaan, että laitteet, ohjelmistot sekä järjestelmän komponentit toimivat liikeprosessien vaatimalla tavalla.

Tarkan testaamisen jälkeen järjestelmän käyttö voidaan aloittaa. Käyttöönoton alussa tulee varmistaa, että ongelmatapauksissa voidaan palata käyttämään vanhoja järjestelmiä. Samalla pitää varmistua, etteivät jo käytössä olevien järjestelmien toiminta vaarannu. Kun uutta järjestelmää aletaan käyttää, keskeytyy järjestelmästä riippuvaiset liiketoimet käyttöönoton ajaksi. Käyttöönottosuunnitelman avulla työn keskeytys saadaan mahdollisimman lyhyt. Suunnitelmassa käydään läpi muun muassa työntekijöiden roolit, sekä järjestys, jossa järjestelmän komponentit otetaan käyttöön ja vanhat otetaan pois käytöstä. Vanhoja järjestelmän osia ei kuitenkaan hävitetä, koska hätätapauksissa voidaan joutua ottamaan vanha järjestelmä takaisin käyttöön. (ISF 2007, SD6)

Järjestelmän käyttöönoton jälkeen suoritetaan järjestelmän käyttöä kartoittava tilannekatsaus, jossa varmistetaan, että järjestelmä toimii tehokkaasti sekä liike-

prosessien vaatimusten mukaisesti. Tarpeen mukaan turvallisuuskontrolleja voidaan muuttaa tietoturvan parantamiseksi. (ISF 2007, 6.3.)

4.6. Loppukäyttäjän ympäristö – End User Environment (UE)

Loppukäyttäjän ympäristöllä tarkoitetaan työntekijöiden pääasiallista työskentely-ympäristöä. Koska työntekijöillä on työtehtäviensä suorittamisen vuoksi pääsy yrityksen arkaluontoisiin materiaaleihin, on materiaalien käsittelyyn liittyvät riskit tunnistettava sekä riskit minimoitava. (ISF 2007, UE.)

4.6.1 Fyysinen turvallisuus

Yrityksen tietovaroista ihmiset ovat tärkeimmät. Siksi työntekijöiden sekä heidän osaamisensa suojaaminen ovat aina turvaamisen ensisijaisina kohteina. Rikkoutuneet laitteet on helppo ja suhteellisen vaivatonta korvata uusilla, mutta ihmisen, ja hänen vuosien kokemuksensa korvaaminen, on vaikeaa. (Andress 2011, 97.)

Fyysisen turvaamisen voi aloittaa määrittelemällä turva-alueet (ISO/IEC 17799:fi 2006, 34). Ulkopuolisten henkilöiden pääsyn estämisellä parannetaan turva-alueiden turvallisuutta. Lukittavat ovat ja ikkunat pitävät useimmat asiattomista henkilöistä toimitilojen ulkopuolella. Videovalvonnalla turvallisuutta lisätään entisestään. (ISF 2007, UE6.4; Andreasson ym. 2013, 51.) Fyysiseen turvallisuuteen kuuluu työympäristön suojaaminen lämmön, veden, lian ja sähkön aiheuttamien riskien varalta (vertaa kohtaa 4.3.1 Laitteiden ja järjestelmien fyysinen suojaaminen). Esimerkiksi ihmisen työympäristön väärä lämpötila laskee työtehoa nopeasti. (Andress 2011, 101-102.)

Kulunvalvonnan avulla voidaan tarkkailla yrityksen tiloissa tapahtuvaa liikkumista. Ulkopuolisten pääsy tiloihin estetään, ja yksilöidyn tunnisteen avulla saadaan tarkat ajat siitä, miten henkilökunta viettää aikaa yrityksen tiloissa. (ISO/IEC 17799:fi 2006, 35)

4.6.2 Ohjelmistojen sekä laitteiden turvallisuus

Yrityksen tulee pitää kirjaa käytössä olevaista tietokoneista, tietokoneissa käytettävistä ohjelmistoista, niiden tuoteavaimista ja lisensseistä sekä käytössä olevista versioista. Merkitsemällä laitteet yksilöllisin merkinnöin, helpotetaan ylläpitoa. Laite- ja ohjelmistoinventaariosta selviää nopeasti yrityksen käytössä olevat laitteet, ohjelmistot sekä laitteiden fyysinen sijainti. Inventaario pidetään ajan tasalla vertaamalla inventaarion sisältöä käytössä oleviin laitteisiin ja ohjelmistoihin määräajoin. Inventaario tulee suojata luvattomalta käytöltä. (ISF 2007, CI1.3)

Työasemina käytettävät tietokoneet tulee suojata viruksilta ja muilta haitakkeilta sopivien ohjelmistojen avulla. Mikäli kone on yhteydessä internetiin, konekohtaisen palomuurin avulla suojataan kone verkkohyökkäyksiltä. (ISF 2007, CI2.4; Andress 2011, 137.)

Ohjelmistojen päivittäminen on tärkeä osa tietoturvaa. Automaattiset päivitykset auttavat päivitysten pitämisessä ajan tasalla. Päivitystarve ei koske vain käyttöjärjestelmiä, vaan myös käytettävien ohjelmistojen pitää olla valmistajan tukemia. Vanhentuneita ohjelmistoja käytetään usein hyväksi tietomurtoja tehtäessä. (Andreasson ym. 2014, 34.)

Muuta laitteiden fyysiseen turvallisuuteen liittyvää tietoa on käyty läpi tarkemmin kohdassa 4.3.1 Laitteiden ja järjestelmien fyysinen suojaaminen.

4.6.3 Varmuuskopiointi

Kuten kriittisiin sovelluksiin ja tietoverkkojen suojaamiseen kuuluu varmuuskopiointi, kuuluu se myös loppukäyttäjien ympäristöissä käytettäviin järjestelmiin. Työpöytäkoneiden, kannettavien tietokoneiden ja siirreltävien muistilaitteiden tiedot tulee varmuuskopioida määräajoin. Varmuuskopiointia tehdessä on varmistuttava siitä että kopioita ei säilytetä vain yhdessä paikassa, vaan yksi kopio

on aina muualla kuin yrityksen tiloissa (ISF, 2007. UE6.3). Näin estetään katastrofaalinen tietojen menetys esimerkiksi vakavan tulipalon sattuessa.

4.6.4 Kirjautuminen ja käyttöoikeudet

Käyttövaltuuksien hallinta on tärkeä osa tietojen suojaamisessa. Pahimmillaan kukaan ei ole selvillä yrityksen järjestelmien käyttöoikeuksista. Tällöin on mahdollista, että täysin ulkopuolisilla henkilöillä pääsy yrityksen tietoihin. Käyttöoikeuspolitiikan avulla yritys voi hallinnoida käyttäjien valtuuttamiseen liittyviä aiheita. Järjestelmien käyttäjien käyttöoikeudet myönnetään työroolien mukaan, ja käyttövaltuudet myönnetään perustellusti työtehtäviin nähden. Käyttöoikeuksien myöntämisen aikaan voidaan käyttäjä velvoittaa allekirjoittamaan käyttö- ja salassapitosopimus. Sopimuksessa tulee käydä läpi järjestelmien käyttöön liittyviä asioita. (Andreasson ym. 2013, 46; Andreasson ym. 2014, 75.)

4.6.5 Tietoaineiston turvallisuus

Työnteossa tarvittavat tietoaineisto on suojattava. Jos yrityksellä on käytössä taulukkolaskenta-taulukoihin perustuvia työkaluja, varmistetaan että käyttäjät eivät voi aiheuttaa väärillä käyttötavoilla vahinkoa taulukoihin. Samoin työympäristössä käytössä olevat tietokannat suojataan. (ISF 2007, UE3.)

Tietoaineistoon liittyvää aiheistoa on käyty tarkemmin läpi kohdassa 4.2.2 Arkaluontoisen materiaalin suojaaminen.

4.6.6 Siirrettävät- ja mobiililaitteet

Älypuhelinten lisääntynyt käyttö aiheuttaa uudenlaisia riskejä. Vaikka asiakassuhteen hoitaminen vapautuu yrityksen toimitiloista riippumattomaksi, riskit lisääntyvät. Yrityksessä on hyvä käydä läpi laitteiden käyttöön liittyviä uhkia. Riskit kasvavat mikäli samalla laitteella tehdään työhön liittyviä tehtäviä ja vapaa-aikaan liittyviä tehtäviä. Selkeiden toimintaperiaatteiden avulla mobiililaitteiden

käytöstä tehdään turvallisempaa. Yrityksen on harkittava hankkiko se työntekijöiden käyttöön vain työasioiden tekemiseen käytettävät laitteet. (Andreasson ym. 2014, 91-92.)

4.6.7 Internetin ja sähköpostin käyttö

Internetin ja sähköpostin käyttö työasioiden hoitoon on lähes välttämätöntä. On kuitenkin hyvä tietää että oletuksena internetissä kulkeva tieto on suojaamatonta. Roskaposti on suuri ongelma. Vaikka lähettäjä näyttää olevan tuttu, voi tili olla kaapattu, tai osoite väärennetty. Kalasteluviesteissä virallisen näköisissä viesteissä pyydetään mahdollisesti kirjautumaan tuttuun palveluun, mutta linkin kautta kirjautumistunnukset päätyvätkin verkkorikollisten käyttöön. Sähköpostin liitetiedostoissa levitetään haittaohjelmia, joten liitetiedostojen avaamisten kanssa on oltava varovaisia. Sähköpostin voi lähettää vahingoksi väärään osoitteeseen, joten on oltava tarkkana että postin lähetys kohdistuu oikeille henkilöille. (ISF 2007, UE5.1; Andreasson ym. 2013, 55-57.)

Pilvipalveluiden käyttö on yleistynyt viime vuosina. Yrityksen on vaikea vaikuttaa ulkopuolisten palveluiden tietoturvaan, mutta palveluiden käyttöön liittyvät periaatteessa samat riskit kuin muidenkin yrityksen verkon ulkopuolisten palveluiden käyttöön. Salatun yhteyden kautta siirretty salakirjoitettu tieto on luottamuksellisuuden ja eheyden suhteen suojattu. Palveluun tallennetun tiedon fyysinen sijainti tosin voi aiheuttaa tietoturvauhan, koska yritys ei voi välttämättä päättää minkälainen lainsäädäntö suojaa palveluun talletettua tietoa (Anderss 2011, 90).

4.6.8 Ohjeistus

Työntekijöille tulee luoda ohjeistus, jossa kerrotaan päivittäisiin työtehtäviin liittyvät riskit, sekä ratkaisuja riskien ehkäisyyn. Tietosuojaan liittyvät asiat pitää lainsäädännön perusteella olla henkilökunnan tiedossa. Ohjeistukseen on hyvä kirjata lisäksi internetin ja sähköpostin käyttöön liittyvää tietoa. Lisäksi sosiaalisen

median käyttöön liittyvää sääntöjä on hyvä sisällyttää ohjeistukseen. Ohjeissa voidaan myös kieltää omien asioiden hoitaminen työpaikan laitteilla. (ISF 2007, UE.)

5 CASE-KARTOITUS, KARTOITUKSEN TULOKSET SEKÄ SUOSITUKSET (SALATTU)

6 POHDINTA

Opinnäytetyön aiheena oli länsisuomalaisen tilitoimiston tietoturvatason kartoittaminen, sekä löytöjen perusteella tietoturvan parantamiseen liittyvien asioiden ehdottaminen. Yrityksen tietoturvan taso saatiin tutkittua, ja löydösten perusteella ehdotettua muutoksia yrityksen toimintatapoihin (kohta 5.2).

Työn aiheen teorian laajuus aiheutti alkuun hankaluuksia. Koska tietoturva ei kuulunut suuntautumisvaihtoehtoni opintoihin, aiheen käytännöt eivät olleet kovin tuttuja. Tutkimalla alaan liittyvää tietoa, perusteet selkiytyivät nopeasti. Tietoturvaan liittyvän teorian selkeydyttyä tajusin, että alkuperäinen tehtävärajaus oli liian laaja. Toimeksiantajalta saatujen suositusten mukaan tehtävä rajattiin paremmin sopimaan yrityksen tarpeita. Kirjanpitoon liittyvää tietoa löytyi hyvin eri lähteistä. Mikäli jokin kirjanpitoon liittynyt asia oli epäselvä, toimeksiantajayrityksen henkilökunta auttoi asioiden selvittämisessä.

Tietoturvan perinteisen kahdeksan osa-alueen jaottelu vaihdettiin kesken teoriaosuuden kirjoittamista ISF:n Standard of Good Practice 2007 -standardin kuuteen osa-alueeseen. SoGP:en vaihto pakotti hankkimaan uutta lähdemateriaalia, joka auttoikin tietoturvaan liittyvien asioiden hahmottamista huomattavasti. Samalla selvisi että SoGP sopii paremmin useista toimipisteistä koostuvien suurten yritysten käyttöön.

Kävin tekemässä kartoitusta yrityksen tiloissa kahteen otteeseen. Ensimmäisen kartoituskerran aikana huomasin, etteivät käytetyt tutkimusmenetelmät olleet tarpeeksi laadukkaat. Vaikka etukäteen ajatellut kysymykset ja tarkastettavat kohteet vaikuttivat riittäviltä, tuli kartoitustilanteessa eteen monta asiaa, joita en ollut osannut ottaa huomioon. Toisella kerralla, paremman kyselylistan avulla, ensimmäisen kartoituksen jälkeen kartoittamatta jääneet asiat saatiin selvitettyä.

Yrityksen toimintaprosesseihin tutustuminen oli opettavaista. Kartoituksen aikana oli mielenkiintoista huomata, miten teoriaosassa käsiteltyjä aiheita voisi liittää

osaksi yrityksen toimintaa. Kartoituksen tulosten perusteella yrityksen tietoturvan tasoa saatiin nostettua sekä tietoturvaan liittyvää tietoutta parannettua.

Ennen opinnäytetyön aloitusta minulla oli mielikuva, että tietoturvarikkeet johtuvat lähinnä tietotekniikkaan liittyvistä seikoista. Aiheeseen liittyvään materiaaliin tutustuessa huomasin, että huono tietoturvallisuusjohtaminen ja huonot käytännöt aiheuttavat ison osan julki tulleista tapauksista. Koska on voitu ajatella tietoturvan olevan yritykselle pelkkä kuluerä, ei tietoturvaan liittyviä käytäntöjä ole osattu toteuttaa aiheen vaatimalla tavalla. Yrityksissä tulisikin päästä eroon ajatuksesta, että tietoturva on kuluerä. Sen sijaan tulisikin lähtökohtaisesti keskittyä kehittämään yrityksen toimintaprosessit tietoturva silmällä pitäen.

LÄHTEET

Andreasson, A; Koivisto, J. & Ylipartanen, A. 2013. Tietosuojavastaavan käsikirja. Helsinki: Tietosanoma.

Andreasson, A; Koivisto, J. & Ylipartanen, A. 2014. Tietosuojavastaavan käsikirja 2. Helsinki: Tietosanoma.

Andress, J. 2011. The Basics of Information Security. Understanding the Fundamentals of InfoSec in Theory and Practice. Waltham: Elsevier.

Bundesamt für Sicherheit in der Informationstechnik, BSI 2014. Information security audit. A guideline for IS audits based on IT-Grundschutz https://www.bsi.bund.de/cae/servlet/contentblob/471376/publicationFile/28211/guideline-isrevision_pdf.pdf viitattu 30.7.2014

CompTIA. 2013. CompTIA 11th Annual Information Security Trends. http://www.slideshare.net/comptia/comptia-11th-annual-information-security-trends Viitattu 28.7.2014

Hachman M. 2011. PlayStation Hack to Cost Sony $171M; Quake Costs Far Higher. Viitattu 10.10.2014 http://www.pcmag.com/article2/0,2817,2385790,00.asp

Henkilötietolaki 22.4.1999/523.

Information Security Forum, ISF 2007. The Standard of Good Practice for Information Security. Viitattu 26.6.2014 https://www.securityforum.org/userfiles/public/2007_sogp_pub.pdf.

ISO/IEC 17799:fi 2006. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintaa koskeva menettelyohje. Helsinki: Suomen Standardoimisliitto.

ISO/IEC 27001:fi 2006. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Helsinki: Suomen Standardisoimisliitto.

ISO/IEC 27001:en 2013. Information technology. Security techniques. Information security management systems. Requirements. Second edition. Geneva:ISO copyright office

Kirjanpitolaki 30.12.1997/1336.

Laakso M. 2010, Tietojesi turvaksi. Tietoturvan osa-alueet. Viitattu 15.10.2014. http://www.tietojesiturvaksi.fi/content/tietoturvan-osa-alueet

Laki yksityisyyden suojasta työelämässä 13.8.2004/759.

Miettinen, M. 2002. Tietoturvan historiaa. Seminaarityö. Tietojenkäsittelyn laitos. Helsinki: Helsingin yliopisto.

Sun Tzu 2007. Sodankäynnin taito. Suom. Karkkolainen, H. Yhdeksäs painos. Helsinki: Tietosanoma Oy.

Suomen Taloushallintoliitto ry 2009. Taloushallintoliitto. Viitattu 12.12.2014 http://www.taloushallintoliitto.fi/taloushallintoliitto/.

Suomen Taloushallintoliitto ry 2011. Kirjanpidon ABC. Viitattu 16.6.2014. http://www.taloushallintoliitto.fi/tilitoimistot/kirjanpidon_abc/.

Tietoturvavaltuutetun toimisto 2012. Laadi tietotilinpäätös. Viitattu 26.11.2014. http://tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6JfpzNVCh/Laadi_tietotilinpaatos.pdf

Tietoturvavaltuutetun toimisto 2014. Ota oppaaksi henkilötietolaki! Viitattu 10.10.2014 http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6Jfq8WnQ7/Ota_oppaaksi_henkilotietolaki.pdf

Tilintarkastuslaki 13.4.2007/459

Valtiovarainministeriö 2007. Tietoturvallisuudella tuloksia.. Viitattu 27.7.2014 https://www.vahtiohje.fi/web/guest/tietoturvallisuudella-tuloksia.

Valtiovarainministeriö 2010. Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta. Tietojen luokittelu. Viitattu 13.10.2014 https://www.vahtiohje.fi/web/guest/tietoaineistojen-luokittelu.

Valtiovarainministeriö 2012. Teknisen ympäristön tietoturvataso-ohje. Suojattavien kohteiden määritteleminen. Viitattu 28.7.2014. https://www.vahtiohje.fi/web/guest/suojattavien-kohteiden-maaritteleminen.

Liite 1. Tietoturvakysely

Turvallisuusjohtaminen:

1. Onko yrityksessä määritetty tietoturvapolitiikka?
2. Onko yrityksen johto sitoutunut turvallisuuspolitiikan ajamiseen?
3. Onko johto sitoutunut turvallisuustavoitteisiin, niiden saavuttamiseen ja jatkuvaan kehittämiseen?
4. Onko turvallisuuspolitiikassa määritetty organisaation keskeiset turvallisuustavoitteet?
5. Onko yrityksessä määritetty tietoturvakäytännöt?
6. Huomioiko turvallisuuskäytännöt lainsäädännön?
7. Onko yrityksellä menetelmät tunnistaa ja arvioida turvallisuusriskit?
8. Onko toiminnalle tärkeät suojattavat kohteet tunnistettu? (mm. tiedot, järjestelmät, prosessit)
9. Arvioidaanko yrityksen tietoturvallisuutta? Miten?
10. Onko alihankkijoiden, palveluntarjoajien ja muiden yhteistyötahojen tietoturvallisuudesta huolehdittu?
11. Onko yrityksellä jatkuvuudenhallintamenettely?
12. Onko organisaatiolla menetelmät turvallisuuspoikkeamien havaitsemiseksi ja suojaamiseksi sekä korjaavien toimenpiteiden tekemiseksi?
13. Miten yrityksessä on huolehdittu riittävästä ohjeistuksesta, koulutuksesta ja tiedotuksesta?
14. Onko henkilöiden taustat selvitetty ja todennettu? (esim. rikosrekisteri, luottotiedot, akateeminen tausta, työhistoria, huumetestaus)
15. Vaaditaanko työntekijöiltä työsopimuksen lisäksi erillisiä sopimuksia? (esim. miten yrityksessä tulee toimia, tiettyjen arvojen noudattaminen, salassapito)
16. Onko turvallisuusvastuut ja -roolit selvitetty henkilöstölle?
17. Toteuttavatko työntekijät turvallisuuspolitiikkaa työssään?
18. Tunteeko henkilöstö omaan työhönsä liittyvät turvallisuusriskit?
19. Vaaditaanko työntekijöiltä turvallisuuspolitiikan toteuttamista osana työtehtäviä?

20. Ovatko työntekijät tietoisia turvallisuuspolitiikasta ja onko heillä selkeä kuva turvallisuuteen liittyvistä velvollisuuksistaan ja vastuistaan?
21. Onko yrityksessä huolehdittu työntekijöiden työtyytyväisyydestä ja -motivaatiosta?
22. Onko yrityksellä menettelyohjeet työsuhteen päättämiselle?
23. Onko avainhenkilöt ja yrityksen riippuvuus heistä tunnistettu?
24. Onko heidän tietämyksensä käytettävyys varmistettu?
25. Onko selvitetty mitkä lait ja määräykset velvoittavat suojaamaan yrityksessä käsiteltävää tietoa?
26. Onko henkilöstön tieoja sisältävät henkilörekisterit suojattu?
27. Onko asiakkaisiin liittyvät arkaluontoiset tiedot suojattu?
28. Onko rekisteriselosteet ajan tasalla ja henkilöiden saatavilla?
29. Onko henkilöstöä ohjeistettu luottamuksellisen ja arkaluontoisen materiaalin käsittelyssä?
30. Onko aineistojen omistajuus ja luokitusvastuut kuvattu?
31. Onko yrityksellä arkistonmuodostussuunnitelma?
32. Huomioiko suunnitelma kaikki tietojärjestelmät ja dokumenttimuodot?
33. Onko asiakirjojen rekisteröintikäytännöt ohjeistettu?
34. Onko huolehdittu että suojattava tieto säilytetään turvallisesti?

Laitteet:

1. Onko kriittiset laitteistot katkottoman sähkönsyötön parissa?
2. Riittääkö varasähköä järjestelmien hallittuun alasajoon?
3. Onko laitteiston toimivuus testattu?
4. Ovatko laitteistot huoltosopimusten tai takuun piirissä?
5. Suoritetaanko laitteistolle säännöllistä huoltoa ja valvontaa?
6. Pidetäänkö laitteista kirjanpitoa/laiterekisteriä?
7. Kirjataanko hävitetty/käytöstä poistettu laite rekisteriin?
8. hävitetäänkö vanhat laitteet asiankuuluvalla tavalla, turvallisesti?

Verkot:

1. Onko verkko dokumentoitu ja ylläpidetäänkö dokumentaatiota?
2. Missä muodossa dokumentointi on?
3. Sisältääkö dokumentointi laitteet, laitteiden käyttämät ohjelmistot ja niiden versiot?
4. Sisältääkö dokumentointi riittävät tiedon laitteiden ja ohjelmistojen oikeista konfiguroinneista?
5. Onko ulkoiset yhteydet rakennettu keskitettyjen pisteiden kautta?
6. Onko verkon eri osat erotettu toisistaan fyysisesti tai loogisesti?
7. Sallitaanko tuntemattomien laitteiden käyttää verkkoa?
8. Käytetäänkö yrityksessä langatonta verkkoa?
9. Miten langattoman verkon turvallinen käyttö varmistetaan?
10. Onko verkon häiriöihin varauduttu?
11. Miten suojattavat tiedot säilytetään tietojärjestelmissä?
12. Voidaanko dokumentaation perusteella siirtää ylläpito tarvittaessa uudelle toimijalle?
13. Onko liikennettä suodattavien laitteiden säännöstöt hyvien tietoturvaperiaatteiden mukaisia?
14. Toimivatko liikennettä suodattavat tai valvovat laitteet halutulla tavalla?
15. Onko laitteet kovennettu?
16. Onko hallintayhteydet suojattu asianmukaisesti?

Loppukäyttäjän ympäristö

1. Onko haittaohjelman torjuntatuotteita käytössä enemmän kuin yksi?
2. Ovatko käyttäjät tietoisia tietoturvallisuuden ja tietosuojan käytölle asettamista vaatimuksista?
3. Voidaanko salasanat vaihtaa hallitusti?

4. Pakotetaanko käyttäjä vaihtamaan salasana määräajoin?
5. Päivittääkö valmistaja käytettäviä ohjelmistoja?
6. Onko ohjelmat versioineen ja lisensseineen listattu?
7. Hallitaanko versioiden vaihtoa?
8. Onko käytössä lokien hallintajärjestelmä?
9. Onko ohjelmien versionhallinta käytössä?
10. Onko yrityksessä olemassa menettely ohjelmistojen päivittämisestä?
11. Onko käyttöoikeudet rajattu työtehtävien vaatimalla tavalla?
12. Ovatko järjestelmät käyttäjäystävällisiä?
13. Onko väliaikaistiedostojen hallinta ja hävittäminen kunnossa?
14. Onko tietojen varmistuskäytännöt vastuutettu ja suunniteltu?
15. Pidetäänkö varmistuksista kirjaa?
16. Säilytetäänkö varmistuksista toisia kopioita muualla?
17. Mikäli tietoja säilytetään muualla kuin yrityksen tiloissa, miten varmistetaan tietojen siirtäminen niin ettei ulkopuoliset pääse tietoihin käsiksi?
18. Onko työasemien virustentorjunta kunnossa?
19. Onko palvelinten virustentorjunta kunnossa?
20. Onko sähköpostin käytöstä laadittu ohjeet?
21. Onko yrityksellä toipumissuunnitelmaa ohjelmistoihin liittyvien ongelmien suhteen?
22. Hävitetäänkö luottamuksellista ja arkaluontoista tietoa sisältävä materiaalia asiaankuuluvalla tavalla?
23. Onko arkistojen palo- ja murtosuojauksesta huolehdittu?
24. Onko arkistotilojen käyttö valvottua?
25. Huolehditaanko ettei kokoustiloihin jää asiakirjoja tai muistiinpanoja kokousten jälkeen?
26. Onko olemassa suunnitelma miten tiedot siirretään vanhasta järjestelmästä uuteen järjestelmään kun nykyinen järjestelmä poistuu käytöstä?
27. Onko laitteet, tiedot ja ohjelmistot kirjattu omaisuusrekisteriin?
28. Onko yrityksessä salattavaa tietoa?

29. Onko salaukseen liittyvät periaatteet koulutettu?
30. Onko salausavainten hallinnasta ohjeistus?
31. Onko salausavainten turvatalletus järjestetty?
32. Onko järjestelmien käyttöoikeuksien hallintaan nimetty vastuuhenkilö?
33. Onko tunnusten huolto hallittua ja dokumentoitua?
34. Onko määritelty ketkä saavat asentaa ohjelmistoja?
35. Onko määritelty mitkä ovat sallittuja ohjelmistoja?
36. Onko jokaisella käyttäjällä oma tunnus ja salasana?
37. Onko tietojärjestelmissä käytössä roolit?
38. Voivatko työntekijät käyttää yrityksen tietojärjestelmiä etänä?
39. Miten etäyhteys on toteutettu?
40. Onko etätyön tekeminen ohjeistettu?
41. Tehdäänkö etätyötä työnantajan antamilla välineillä?
42. Saako etätyötä tehdä muilla kuin työnantajan antamilla välineillä?
43. Onko tietokoneiden henkilökohtainen käyttö työaikana sallittua?
44. Onko henkilökohtainen käyttö ohjeistettua?
45. Saako työhön liittyvää materiaalia viedä pois työpaikalta?
46. Onko olemassa käytännöt, joilla erotetaan yksityinen ja työnantajan aineisto toisistaan?
47. Miten varmistetaan että verkossa ja sen palveluissa ei ole tunnettuja haavoittuvuuksia?
48. Miten varmistetaan ettei ulkopuoliset pääse käyttämään valvomattomia laitteita?
49. Onko yrityksessä voimassa ns. puhtaan pöydän ja/tai tyhjän ruudun politiikka?
50. Onko tulostimille pääsy rajoitettu?
51. Onko varmistettu ettei työntekijälle synny ns. vaarallisia työyhdistelmiä?
52. Voiko yksi henkilö peittää luvattoman toimintansa jäljet?
53. Ovatko neuvottelutilat ääni- ja näköeristettyjä?
54. Onko varauduttu teknisten järjestelmien rikkoutumiseen?

55. Onko tekninen ympäristö, eli laitteisto, ja sen muutokset dokumentoitu?
56. Onko toimitilat jaettu tärkeyden mukaan erilaisiin turva-alueisiin?
57. Miten asiattomien henkilöiden pääsy suojattuihin tiloihin estetään?
58. Kenellä on oikeus päästä suojattuun tilaan?
59. Sijaitsevatko tietojen kannalta kriittiset laitteet (esim. serverit ja palomuurit) suojatuissa tiloissa?
60. Onko henkilöiden kulkuoikeudet yksilöity (esim. kulkulätkän avulla)?
61. Onko mekaanisten avainten hallinta järjestetty?
62. Onko tiloihin yleisavaimia? Kenellä avaimet ovat ja kuka vastaa avaimista?
63. Onko tiloissa rikosilmoitinjärjestelmä?
64. Onko tiloissa kulunvalvonta?
65. Onko tiloissa kameravalvonta?
66. Miten edellä mainittuja järjestelmiä hallinnoidaan?